

Aviso de
CONTRATAÇÃO DIRETA

Nº 0017/2024

CONTRATANTE (UASG)

996612 – CONSELHO REGIONAL DE CONTABILIDADE DO PARÁ

OBJETO

Aquisição das licenças de uso da solução de segurança antivírus Kaspersky Next EDR Foundations para estações de trabalho (endpoints), servidores e dispositivos móveis, gerenciados por solução centralizada no modelo on-premise, contemplando o serviço de implantação, com repasse de instrução e orientação técnica referente a manutenção preventiva, além da garantia, suporte técnico do fabricante e atualizações por 36 (trinta e seis) meses.

VALOR TOTAL DA CONTRATAÇÃO

R\$ 19.085,23

DATA DA SESSÃO

DIA: 13/11/2024

HORÁRIO DA FASE DE LANCES

Das 10h até as 16h

CRITÉRIO DE JULGAMENTO:

Menor preço por item

**PREFERÊNCIA ME/EPP/EQUIPARADAS
SIM**

Sumário

- [1. OBJETO DA CONTRATAÇÃO DIRETA](#)
- [2. PARTICIPAÇÃO NA DISPENSA ELETRÔNICA.](#)
- [3. INGRESSO NA DISPENSA ELETRÔNICA E CADASTRAMENTO DA PROPOSTA INICIAL](#)
- [4. FASE DE LANCES](#)
- [5. JULGAMENTO E ACEITAÇÃO DAS PROPOSTAS](#)
- [6. HABILITAÇÃO](#)
- [7. CONTRATAÇÃO](#)
- [8. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS](#)
- [9. DAS DISPOSIÇÕES GERAIS](#)

CONSELHO REGIONAL DE CONTABILIDADE DO PARÁ

AVISO DE CONTRATAÇÃO DIRETA Nº 017/2024

(Processo Administrativo n.º 9079612110000416.000012/2024-81)

Torna-se público que o CONSELHO REGIONAL DE CONTABILIDADE, por meio do Setor de Licitações e Contratos, realizará Dispensa Eletrônica, com critério de julgamento (*menor preço*), na hipótese do [art. 75, inciso II](#), nos termos da [Lei n.º 14.133, de 1º de abril de 2021](#), da [Instrução Normativa Seges/ME nº 67, de 2021](#), e demais normas aplicáveis.

Data da sessão: 13/11/2024

Horário da Fase de Lances: 10h às 16h

Link: www.gov.br/compras

Critério de Julgamento: menor preço

1. OBJETO DA CONTRATAÇÃO DIRETA

- 1.1. O objeto do presente procedimento é a escolha da proposta mais vantajosa para a contratação, por dispensa de licitação, de Aquisição das licenças de uso da solução de segurança antivírus Kaspersky Next EDR Foundations para estações de trabalho (endpoints), servidores e dispositivos móveis, gerenciados por solução centralizada no modelo on-premise, contemplando o serviço de implantação, com repasse de instrução e orientação técnica referente a manutenção preventiva, além da garantia, suporte técnico do fabricante e atualizações por 36 (trinta e seis) meses, conforme condições, quantidades e exigências

estabelecidas neste Aviso de Contratação Direta e seus anexos.

1.1.1. Havendo mais de um item, faculta-se ao fornecedor a participação em quantos forem de seu interesse.

1.2. O critério de julgamento adotado será o *menor preço*, observadas as exigências contidas neste Aviso de Contratação Direta e seus Anexos quanto às especificações do objeto.

2. PARTICIPAÇÃO NA DISPENSA ELETRÔNICA.

2.1. A participação na presente dispensa eletrônica ocorrerá por meio do Sistema de Dispensa Eletrônica, ferramenta informatizada integrante do Sistema de Compras do Governo Federal – Compras.gov.br, disponível no Portal de Compras do Governo Federal, no endereço eletrônico www.gov.br/compras.

2.1.1. O procedimento será divulgado no Compras.gov.br e no [Portal Nacional de Contratações Públicas - PNCP](#), e encaminhado automaticamente aos fornecedores registrados no Sistema de Registro Cadastral Unificado - Sicaf, por mensagem eletrônica, na correspondente linha de fornecimento que pretende atender.

2.1.2. O Compras.gov.br poderá ser acessado pela web ou pelo [aplicativo Compras.gov.br](#).

2.1.3. O fornecedor é o responsável por qualquer transação efetuada diretamente ou por seu representante no Sistema de Dispensa Eletrônica, não cabendo ao provedor do Sistema ou ao órgão entidade promotor do procedimento a responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros não autorizados.

2.2. *Para o item 1, a participação é exclusiva a microempresas e empresas de pequeno porte, nos termos do art. 49, inciso IV, c/c o art. 48, inciso I, da Lei Complementar nº 123, de 14 de dezembro de 2006.*

2.2.1. *A obtenção do benefício a que se refere o item anterior fica limitada às microempresas e às empresas de pequeno porte que, no ano-calendário de realização do procedimento, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.*

2.2.2. *Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021, para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto n.º 8.538, de 2015.*

2.3. Não poderão participar desta dispensa de licitação os fornecedores:

2.3.1. que não atendam às condições deste Aviso de Contratação Direta e seu(s) anexo(s);

2.3.2. estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

2.3.3. que se enquadrem nas seguintes vedações:

a) autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a contratação versar sobre obra, serviços ou fornecimento de bens a ele relacionados;

b) empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a contratação versar sobre obra, serviços ou fornecimento de bens a ela necessários;

c) pessoa física ou jurídica que se encontre, ao tempo da contratação, impossibilitada de contratar em decorrência de sanção que lhe foi imposta;

d) aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na dispensa de licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

e) empresas controladoras, controladas ou coligadas, nos termos da [Lei nº 6.404, de 15 de dezembro de 1976](#), concorrendo entre si;

f) pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do aviso, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista.

2.3.3.1. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico;

2.3.3.2. O disposto na alínea “c” aplica-se também ao fornecedor que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do fornecedor;

2.3.4. organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário); e

2.3.5. *sociedades cooperativas*.

2.4. Não poderá participar, direta ou indiretamente, da dispensa eletrônica ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme [§ 1º do art. 9º da Lei n.º 14.133, de 2021](#).

3. INGRESSO NA DISPENSA ELETRÔNICA E CADASTRAMENTO DA PROPOSTA INICIAL

3.1. O ingresso do fornecedor na disputa da dispensa eletrônica ocorrerá com o cadastramento de sua proposta inicial, na forma deste item.

3.2. O fornecedor interessado, após a divulgação do Aviso de Contratação Direta, encaminhará, exclusivamente por meio do Sistema de Dispensa Eletrônica, a proposta com a descrição do objeto ofertado, a marca do produto, quando for o caso, e o preço ou o desconto, até a data e o horário estabelecidos para abertura do procedimento.

3.2.1. *O fornecedor não poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação.*

3.3. Todas as especificações do objeto contidas na proposta, em especial o preço ou o desconto ofertado, vinculam a Contratada.

3.4. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto;

3.4.1. A proposta deverá conter declaração de que compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

3.4.2. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do fornecedor, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

3.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será aquela correspondente à média dos efetivos recolhimentos da empresa nos últimos doze meses.

3.6. Independentemente do percentual do tributo que constar da planilha, no pagamento serão retidos na fonte os percentuais estabelecidos pela legislação vigente.

3.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar os serviços nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo,

quando requerido, sua substituição.

3.8. O prazo de validade da proposta não será inferior a 60 dias (sessenta) dias , a contar da data de sua apresentação.

3.9. No cadastramento da proposta inicial, o fornecedor deverá, também, assinalar Termo de Aceitação, em campo próprio do sistema eletrônico, relativo às seguintes declarações:

3.9.1. que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

3.9.2. que está ciente e concorda com as condições contidas no Aviso de Contratação Direta e seus anexos;

3.9.3. que se responsabiliza pelas transações que forem efetuadas no sistema, assumindo-as como firmes e verdadeiras;

3.9.4. que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, de que trata [o art. 93 da Lei nº 8.213/91](#) .

3.9.5. que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do [artigo 7º, XXXIII, da Constituição](#);

3.10. O fornecedor organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no [artigo 16 da Lei nº 14.133, de 2021](#).

3.11. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no [artigo 3º da Lei Complementar nº 123, de 2006](#) , estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos [§§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021](#).

3.12. *Desde que disponibilizada a funcionalidade no sistema, fica facultado ao fornecedor, ao cadastrar sua proposta inicial, a parametrização de valor final mínimo, com o registro do seu lance final aceitável (menor preço ou maior desconto, conforme o caso).*

3.12.1. *Feita essa opção os lances serão enviados automaticamente pelo sistema, respeitados os limites cadastrados pelo fornecedor e o intervalo mínimo entre lances previsto neste aviso.*

3.12.1.1. *Sem prejuízo do disposto acima, os lances poderão ser enviados manualmente, na forma da seção respectiva deste Aviso de Contratação Direta;*

3.12.2. *O valor final mínimo poderá ser alterado pelo fornecedor durante a fase de disputa, desde que não assuma valor superior a lance já registrado por ele no sistema.*

3.12.3. *O valor mínimo parametrizado possui caráter sigiloso aos demais participantes do certame e para o órgão ou entidade contratante. Apenas os lances efetivamente enviados poderão ser conhecidos dos fornecedores na forma da seção seguinte deste Aviso.*

4. FASE DE LANCES

41. A partir da data e horário estabelecidos neste Aviso de Contratação Direta, a sessão pública será automaticamente aberta pelo sistema para o envio de lances públicos e sucessivos, exclusivamente por meio do sistema eletrônico, sendo encerrado no horário de finalização de lances também já previsto neste aviso.

42. Iniciada a etapa competitiva, os fornecedores deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

4.2.1. O lance deverá ser ofertado pelo *valor unitário* do item.

43. O fornecedor somente poderá oferecer valor inferior ou percentual de desconto superior ao último lance por ele ofertado e registrado pelo sistema.

4.3.1. O fornecedor poderá oferecer lances sucessivos iguais ou superiores ao lance que esteja vencendo o certame, desde que inferiores ao menor por ele ofertado e registrado pelo sistema, sendo tais lances

definidos como “lances intermediários” para os fins deste Aviso de Contratação Direta.

4.3.2. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao que cobrir a melhor oferta é de 0,25 (*vinete e cinco centésimos*).

44. Havendo lances iguais ao menor já ofertado, prevalecerá aquele que for recebido e registrado primeiro no sistema.
45. Caso o fornecedor não apresente lances, concorrerá com o valor de sua proposta.
46. Durante o procedimento, os fornecedores serão informados, em tempo real, do valor do menor lance ou do maior desconto registrado, vedada a identificação do fornecedor.
47. Imediatamente após o término do prazo estabelecido para a fase de lances, haverá o seu encerramento, com o ordenamento e divulgação dos lances, pelo sistema, em ordem crescente de classificação.
 - 4.7.1. O encerramento da fase de lances ocorrerá de forma automática pontualmente no horário indicado, sem qualquer possibilidade de prorrogação e não havendo tempo aleatório ou mecanismo similar.

5. JULGAMENTO E ACEITAÇÃO DAS PROPOSTAS

- 5.1. Encerrada a fase de lances, quando a proposta do primeiro colocado permanecer acima do preço máximo ou abaixo do desconto definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas.
 - 5.1.1. Neste caso, será encaminhada contraproposta ao fornecedor que tenha apresentado o menor preço ou o maior desconto, para que seja obtida a melhor proposta compatível em relação ao estipulado pela Administração.
 - 5.1.2. A negociação poderá ser feita com os demais fornecedores classificados, exclusivamente por meio do sistema, respeitada a ordem de classificação, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo ou abaixo do desconto definido para a contratação.
- 5.2. Em qualquer caso, concluída a negociação, se houver, o resultado será divulgado a todos e registrado na ata do procedimento da dispensa eletrônica, devendo esta ser anexada aos autos do processo de contratação.
- 5.3. Constatada a compatibilidade entre o valor da proposta e o estipulado para a contratação, será solicitado ao fornecedor o envio da proposta adequada ao último lance ofertado ou ao valor negociado, se for o caso, acompanhada dos documentos complementares, quando necessários.
 - 5.3.1. *Além da documentação supracitada, o fornecedor com a melhor proposta deverá encaminhar planilha com indicação de custos unitários e formação de preços, com os valores adequados à proposta vencedora.*
- 5.4. Encerrada a etapa de negociação, se houver, o pregoeiro verificará se o fornecedor provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e nos itens 3.3 e seguintes deste Aviso, especialmente quanto à existência de sanção que impeça a participação no processo de contratação direta ou a futura contratação, mediante a consulta aos seguintes cadastros:
 - 5.4.1. SICAF;
 - 5.4.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sanções/ceis>); e
 - 5.4.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sanções/cnep>).
- 5.5. A consulta aos cadastros será realizada em nome da empresa fornecedora e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei nº 8.429, de 1992.
- 5.6. Caso conste na Consulta de Situação do fornecedor a existência de Ocorrências Impeditivas Indiretas, o órgão diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de

Ocorrências Impeditivas Indiretas. (IN nº 3/2018, art. 29, caput)

- 5.6.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (IN nº 3/2018, art. 29, §1º).
- 5.6.2. O fornecedor será convocado para manifestação previamente a uma eventual desclassificação. (IN nº 3/2018, art. 29, §2º).
- 5.6.3. Constatada a existência de sanção, o fornecedor será reputado inabilitado, por falta de condição de participação.
- 5.7. Verificadas as condições de participação, o gestor examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Aviso de Contratação Direta e em seus anexos.
- 5.8. Será desclassificada a proposta vencedora que:
 - 5.8.1. contiver vícios insanáveis;
 - 5.8.2. não obedecer às especificações técnicas pormenorizadas neste aviso ou em seus anexos;
 - 5.8.3. apresentar preços inexequíveis ou que permanecerem acima do preço máximo definido para a contratação;
 - 5.8.4. não tiver sua exequibilidade demonstrada, quando exigido pela Administração;
 - 5.8.5. apresentar desconformidade com quaisquer outras exigências deste aviso ou seus anexos, desde que insanável.
- 5.9. Quando o fornecedor não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contento o objeto, será considerada inexequível a proposta de preços ou menor lance que:
 - 5.9.1. for insuficiente para a cobertura dos custos da contratação, apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da dispensa não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio fornecedor, para os quais ele renuncie a parcela ou à totalidade da remuneração.
 - 5.9.2. apresentar um ou mais valores da planilha de custo que sejam inferiores àqueles fixados em instrumentos de caráter normativo obrigatório, tais como leis, medidas provisórias e convenções coletivas de trabalho vigentes.
- 5.10. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que o fornecedor comprove a exequibilidade da proposta.
- 5.11. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço.
 - 5.11.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;
 - 5.11.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.
- 5.12. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.
- 5.13. Se a proposta ou lance vencedor for desclassificado, será examinada a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.
- 5.14. Havendo necessidade, a sessão será suspensa, informando-se no “chat” a nova data e horário para a sua continuidade.
- 5.15. Encerrada a análise quanto à aceitação da proposta, será iniciada a fase de habilitação, observado o disposto neste Aviso de Contratação Direta.

6. HABILITAÇÃO

- 6.1. Os documentos a serem exigidos para fins de habilitação, **nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021**, constam do Termo de Referência e serão solicitados do fornecedor mais bem classificado na fase de lances.
- 6.2. A habilitação dos fornecedores será verificada por meio do SICAF, nos documentos por ele abrangidos.
 - 6.2.1. É dever do fornecedor atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, quando solicitado, a respectiva documentação atualizada.
 - 6.2.2. O descumprimento do subitem acima implicará a inabilitação do fornecedor, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões lograr êxito em encontrar a(s) certidão(ões) válida(s).
- 6.3. Na hipótese de necessidade de envio de documentos complementares, indispensáveis à confirmação dos já apresentados para a habilitação, ou de documentos não constantes do SICAF, o fornecedor será convocado a encaminhá-los, em formato digital, por meio do sistema, no prazo de 2 horas sob pena de inabilitação. ([art. 19, § 3º, da IN Seges/ME nº 67, de 2021](#)).
- 6.4. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital.
- 6.5. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.
- 6.6. Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.
- 6.7. Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.
- 6.8. Havendo necessidade de analisar minuciosamente os documentos exigidos, a sessão será suspensa, sendo informada a nova data e horário para a sua continuidade.
- 6.9. Será inabilitado o fornecedor que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Aviso de Contratação Direta.
 - 6.9.1. Na hipótese de o fornecedor não atender às exigências para a habilitação, o órgão ou entidade examinará a proposta subsequente, e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda às especificações do objeto e as condições de habilitação
- 6.10. Constatado o atendimento às exigências de habilitação, o fornecedor será habilitado.

7. CONTRATAÇÃO

- 7.1. Após a homologação e adjudicação, caso se conclua pela contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.
- 7.2. O adjudicatário terá o prazo de 3 (três) dias úteis, contados a partir da data de sua convocação, para *assinar o Termo de Contrato*, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste Aviso de Contratação Direta.
 - 7.2.1. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato, a Administração poderá encaminhá-lo para assinatura, mediante correspondência postal com aviso de recebimento (AR), disponibilização de acesso à sistema de processo eletrônico para esse fim ou outro meio eletrônico, para que seja assinado e devolvido no prazo de 3 (três) dias, a contar da data de seu recebimento ou da disponibilização do acesso ao sistema de processo eletrônico.
 - 7.2.2. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.
- 7.3. O prazo de vigência da contratação é o estabelecido no Termo de contrato.
- 7.4. Na assinatura do contrato ou do instrumento equivalente será exigida a comprovação das condições de habilitação e contratação consignadas neste aviso, que deverão ser mantidas pelo fornecedor durante a

vigência do contrato.

8. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

8.1. Comete infração administrativa o fornecedor que praticar quaisquer das hipóteses previstas no [art. 155 da Lei nº 14.133, de 2021](#), quais sejam:

- 8.1.1. dar causa à inexecução parcial do contrato;
- 8.1.2. dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
- 8.1.3. dar causa à inexecução total do contrato;
- 8.1.4. deixar de entregar a documentação exigida para o certame;
- 8.1.5. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
- 8.1.6. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
- 8.1.7. ensejar o retardamento da execução ou da entrega do objeto da contratação direta sem motivo justificado;
- 8.1.8. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;
- 8.1.9. fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;
- 8.1.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
 - 8.1.10.1. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.
- 8.1.11. praticar atos ilícitos com vistas a frustrar os objetivos deste certame.

8.1.12. praticar ato lesivo previsto no [art. 5º da Lei nº 12.846, de 1º de agosto de 2013](#).

8.2. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

- a) Advertência pela falta do subitem 8.1.1 deste Aviso de Contratação Direta, quando não se justificar a imposição de penalidade mais grave;
- b) Multa de 5% (cinco por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor, por qualquer das infrações dos subitens 8.1.1 a 8.1.12;
- c) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, nos casos dos subitens 8.1.2 a 8.1.7 deste Aviso de Contratação Direta, quando não se justificar a imposição de penalidade mais grave;
- d) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 8.1.8 a 8.1.12, bem como nos demais casos que justifiquem a imposição da penalidade mais grave;

8.3. A aplicação das sanções previstas neste Aviso de Contratação Direta não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Contratante ([art. 156, §9º](#))

8.4. Todas as sanções previstas neste Aviso poderão ser aplicadas cumulativamente com a multa ([art. 156, §7º](#)).

8.5. Antes da aplicação da multa, será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação ([art. 157](#))

8.6. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente ([art. 156, §8º](#)).

8.7. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (*trinta*) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

8.8. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no **caput** e parágrafos do [art. 158 da Lei nº 14.133, de 2021](#), para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

8.9. Na aplicação das sanções serão considerados ([art. 156, §1º](#)):

8.10. a natureza e a gravidade da infração cometida;

8.11. as peculiaridades do caso concreto;

8.12. as circunstâncias agravantes ou atenuantes;

8.13. os danos que dela provierem para o Contratante;

8.14. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

8.15. Os atos previstos como infrações administrativas na [Lei nº 14.133, de 2021](#), ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na [Lei nº 12.846, de 1º de agosto de 2013](#), serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei ([art. 159](#)).

8.16. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia ([art. 160](#))

8.17. O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ele aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. ([Art. 161](#))

8.18. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do [art. 163 da Lei nº 14.133, de 2021](#).

8.19. As sanções por atos praticados no decorrer da contratação estão previstas nos anexos a este Aviso.

9. DAS DISPOSIÇÕES GERAIS

9.1. No caso de todos os fornecedores restarem desclassificados ou inabilitados (procedimento fracassado), a Administração poderá:

9.1.1. republicar o presente aviso com uma nova data;

9.1.2. valer-se, para a contratação, de proposta obtida na pesquisa de preços que serviu de base ao procedimento, se houver, privilegiando-se os menores preços, sempre que possível, e desde que atendidas às condições de habilitação exigidas.

9.1.2.1. No caso do subitem anterior, a contratação será operacionalizada fora deste procedimento.

9.1.3. fixar prazo para que possa haver adequação das propostas ou da documentação de habilitação, conforme o caso.

9.2. As providências dos subitens 9.1.1 e 9.1.2 também poderão ser utilizadas se não houver o comparecimento de quaisquer fornecedores interessados (procedimento deserto).

9.3. Havendo a necessidade de realização de ato de qualquer natureza pelos fornecedores, cujo prazo não conste deste Aviso de Contratação Direta, deverá ser atendido o prazo indicado pelo agente competente da Administração na respectiva notificação.

9.4. Caberá ao fornecedor acompanhar as operações, ficando responsável pelo ônus decorrente da perda do negócio diante da inobservância de quaisquer mensagens emitidas pela Administração ou de sua desconexão.

9.5. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário.

9.6. Os horários estabelecidos na divulgação deste procedimento e durante o envio de lances observarão o horário de Brasília-DF, inclusive para contagem de tempo e registro no Sistema e na documentação relativa ao procedimento.

9.7. No julgamento das propostas e da habilitação, a Administração poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

9.8. As normas disciplinadoras deste Aviso de Contratação Direta serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

9.9. Os fornecedores assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo de contratação.

9.10. Em caso de divergência entre disposições deste Aviso de Contratação Direta e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Aviso.

9.11. Da sessão pública será divulgada Ata no sistema eletrônico.

9.12. Integram este Aviso de Contratação Direta, para todos os fins e efeitos, os seguintes anexos:

9.12.1. ANEXO I – Termo de Referência

9.12.1.1. ANEXO I – Especificação Técnica

9.12.1.2. ANEXO I.1 - Estudo Técnico Preliminar Especificação Técnica

9.12.2. ANEXO - A - MODELO DE ORDEM DE SERVIÇO

9.12.3. ANEXO - B - TERMO DE SIGILO (0469131)

9.12.4. ANEXO - C - INSTRUMENTO DE MEDIÇÃO DE RESULTADOS (IMR)

9.12.5. ANEXO - D - MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO

9.12.6. ANEXO - E - MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

9.12.7. ANEXO II - Minuta de Contrato

Belém-PA, 08 de novembro de 2024

AILTON RAMOS
CORREA
JUNIOR:67796486200

Assinado de forma digital por
AILTON RAMOS CORREA
JUNIOR:67796486200
Dados: 2024.11.08 10:17:33 -03'00'

AILTON RAMOS CORREA JUNIOR
Presidente do CRCPA



CONSELHO REGIONAL DE CONTABILIDADE DO PARÁ
Rua Avertano Rocha, 392, - Bairro Comércio, Belém/PA, CEP 66023-120
Telefone: (91) 3202-4150 - www.crcpa.org.br E-mail: crcpa@crcpa.org.br

NLL - TERMO DE REFERENCIA DE TIC

Processo nº 9079612110000416.000012/2024-81

LEI 14.133/2021

(Processo nº 34/2023 - COM)

Referência: Arts. 12 a 24 da Instrução Normativa SGD/ME nº 94, de 2022

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Aquisição das licenças de uso da solução de segurança antivírus Kaspersky Next EDR Foundations para estações de trabalho (endpoints), servidores e dispositivos móveis, gerenciados por solução centralizada no modelo on-premise, contemplando o serviço de implantação, com repasse de instrução e orientação técnica referente a manutenção preventiva, além da garantia, suporte técnico do fabricante e atualizações por 36 (trinta e seis) meses.

DESCRIÇÃO/ ESPECIFICAÇÃO	IDENTIFICAÇÃO CATSERV/ CATMAT	UNIDADE DE MEDIDA	QUANTIDADE
Licença de uso Kaspersky Next EDR Foundations Brazilian Edition 36 Meses instalação/implantação - Suporte do fabricante	26077	Quantidade	70

1.2. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

1.3. Havendo divergência entre o código CATMAT e/ou a descrição do material do Sistema Compras Governamentais, com o apresentado neste Termo de Referência, prevalecerá o último, salvo disposição expressa do CRCPA;

1.4. Os quantitativos e respectivos códigos dos itens são os discriminados na tabela do item 2.1.1.;

1.5. Os bens objetos desta contratação são caracterizados como comum continuado;

1.6. O prazo de vigência do contrato é de 36 (trinta e seis) meses, contados da assinatura do contrato, podendo ser prorrogável para até 10 anos, na forma dos artigos [106 e 107 da Lei nº 14.133, de 2021](#) por interesse das partes.

1.7. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

1.8. A presente contratação adotará como regime de execução a Empreitada por Preço Global;

1.9. A contratada deverá fornecer as licenças em sua versão mais atual.

2. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO ESPECIFICAÇÃO DO PRODUTO

2.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

2.2. O uso de sistemas informatizados tornou-se imprescindíveis ao desenvolvimento das atividades tanto da Administração Pública quanto da iniciativa privada, servindo de base à prestação de inúmeros serviços.

2.2.1. Nesse sentido, a fim de desenvolver as atividades diárias do CRCPA com eficiência, agilidade e segurança, se faz necessário a contratação de Subscrição de licenças de uso da solução de segurança antivírus Kaspersky Next EDR Foundations Brazilian Edition , por 36 (trinta e seis) meses, para 65 usuários 5 servidores.

2.2.2. A solução deve ser do tipo endpoint, além disso, deverá ser capaz de gerir políticas de segurança distintas, visto que existem demandas personalizadas de acordo com as necessidades de usuários específicos e deve conter funcionalidades essenciais à segurança tais como: firewall, políticas de acesso a websites, bloqueio de transmissão de informações sensíveis e acesso a informações avançadas sobre as ações executadas, para que assim se possa realizar auditorias referentes a possíveis danos ao ambiente computacional do Conselho Regional de Contabilidade do Estado do Pará - CRCPA.

2.2.3. Deve possuir uma plataforma para gerenciamento de configurações e ajustes relacionados ao endpoint. Essa plataforma deverá possuir características essenciais como o envio de relatório (por e-mail) referenciando o uso das funcionalidades da solução (websites e aplicações bloqueadas e atividades referentes ao firewall). Deverá ainda possuir dashboard personalizável com as informações que existem maior atenção, tais como: níveis de ameaça e quantidade de riscos. Além disso, a plataforma deverá fornecer atualizações de políticas - via rede -, fornecer capacidade de agregar múltiplos dispositivos em diferentes unidades organizacionais, garantindo assim maior eficácia na adoção de medidas personalizadas de segurança.

2.2.4. O endpoint deve ser capaz de analisar as ações tomadas pelo usuário e identificar possíveis incidentes que afetem a rede de computadores.

2.2.5. A solução deverá ser capaz de remover outras soluções que ajam de maneira concomitante com a mesma.

2.2.6. O endpoint também deverá possuir controles relacionados à permissibilidade, para que apenas usuários administradores possam realizar configurações e ajustes manuais.

2.2.7. Deverá realizar varreduras em unidades externas (ex: USB) que venham a se conectar com o dispositivo e, caso necessário, adotar medidas para o bloqueio de atividades suspeitas.

2.2.8. Portanto, com a contratação espera-se aprimorar a política de segurança, completa com um conjunto de medidas essenciais para modernização da Rede de Dados do Conselho. Com intuito de entregar aos usuários finais, maior confiabilidade, credibilidade e robustez, essa aquisição almeja na continuidade da capacidade de abranger as necessidades de visibilidade total nos eventos e ameaças de segurança. O Conselho Regional de Contabilidade do Pará (CRCPA), continuamente, busca manter seus equipamentos de informática atualizados visando aprimorar e agilizar o trabalho de seu corpo funcional e dos que dependem de utilizar os equipamentos e sistemas do órgão. Além de atender às alterações na Lei 4.320 de 17 de Março de 1964 quanto à Contabilidade aplicada ao Setor Público, os módulos deverão atender às exigências legais das novas regras estabelecidas pela Portaria STN 749 de 15 de Dezembro de 2009 e STN 751 de 16 de Dezembro de 2009, e, principalmente, as diretrizes abaixo discriminadas, contidas nos Manuais de Contabilidade Aplicada ao Setor Público (MCASP), atualizados pela Portaria STN 406 de 20/06/2011 e posteriores.

2.3. A quantidade do que se pretende adquirir, conts ano quadro abaixo:

ID	DESCRIÇÃO/ ESPECIFICAÇÃO	IDENTIFICAÇÃO CATSERV	UNIDADE DE MEDIDA	QUANTIDADE DE EQUIPAMENTOS
----	--------------------------	--------------------------	----------------------	-------------------------------

1	Licença de uso Kaspersky Next EDR Foundations Brazilian Edition 36 Meses instalação/implantação - Suporte do fabricante	26077	Quantidade	70 licenças
---	--	-------	------------	-------------

2.4. MANUAIS/ TUTORIAIS (Caso necessário)

2.4.1. Apresentar, quando da entrega do objeto, os manuais básicos de instruções de uso e de recursos de operação dos equipamentos, escritos em língua portuguesa;

2.4.2. Todos os sistemas deverão ser entregues com os respectivos manuais e ou tutoriais de operação com todas as especificações que possibilitem seu uso pelos funcionários do CRCPA.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. A presente contratação justifica-se e em decorrência da finalidade e dar continuidade a segurança dos computadores, notebooks e servidores atrelados a rede de informática deste Conselho Regional de Contabilidade do Pará – CRCPA. A contratação é necessária devido o vencimento da licença de uso do Antivírus, que finda no dia 09/09/2024, sendo assim, para evitar os riscos das constantes ameaças de segurança e priorizando a segurança da organização do CRCPA, em decorrência da evolução tecnológica, é necessário a contratação deste serviço para que o setor de Tecnologia da Informação deste Regional, gerencie e administre de forma eficiente esta segurança, que demanda a utilização de ferramentas adequadas e modernas. A fim de, minimizar os riscos de acesso indevidos a conteúdo duvidoso, que possa comprometer o funcionamento de determinados dispositivos e conseqüentemente o roubo de informações geradas no ambiente tecnológico.

Com a contratação espera-se aprimorar a política de segurança, completa com um conjunto de medidas essenciais para modernização da Rede de Dados do Conselho. Com intuito de entregar aos usuários finais, maior confiabilidade, credibilidade e robustez, essa aquisição almeja ser capaz de abranger as necessidades de visibilidade total nos eventos e ameaças de segurança. O Conselho Regional de Contabilidade do Pará (CRCPA), continuamente, busca manter seus equipamentos de informática atualizados visando aprimorar e agilizar o trabalho de seu corpo funcional e dos que dependem de utilizar os equipamentos e sistemas do órgão.

Destaca-se que a iniciativa está prevista no Plano Diretor de Tecnologia da Informação - PDTI 2024-2025 deste Conselho Regional de Contabilidade do Pará aprovada e Fevereiro de 2024.

Considerando os objetivos estratégicos e as necessidades corporativas do Conselho Regional de Contabilidade do Pará, bem como o seu alinhamento ao PDTI e ao Plano Anual de Contratações, a aquisição de softwares arquitetônicos e técnicos para o CRCPA tem como objetivo atender às necessidades de manutenção predial e se alinha à Resolução CFC 1.543/2018, que aprova o planejamento estratégico do Sistema CFC/CRCs para 2018/2027, em seu objetivo n.º 15 “Assegurar adequada infraestrutura e suporte logístico às necessidades do Sistema CFC/CRC´s.”.

Portanto, é necessário frisar que, tão importante quanto efetuar a presente contratação, é garantir que a mesma atenda aos melhores critérios técnicos sinalizados pelo mercado de Tecnologia da Informação, respeitando os princípios da economicidade, eficiência e eficácia de grande relevância para as ações governamentais, ao mesmo tempo em que subsidia a disponibilidade dos serviços de TI.

3.2. O objeto da contratação está previsto no Plano de Contratações Anual 2024, conforme detalhamento a seguir:

ALINHAMENTO AO PDTI – Biênio 2024/2025			
ID	Ação do PDTIC	ID	Meta do PDTIC associada

10	Aditar ou contratar empresa especializada para implantação./ Adquirir licenças de uso de software. Manter treinado o corpo funcionou da TI.	10	Implementar com garantia licenças de uso de software antivírus para estações de trabalho e, servidores da rede, em modalidade de licenciamento, com garantia de no mínimo de 36 meses.
ALINHAMENTO AO PCA – 2024			
Item		Descrição	
71		Aquisição de licenças Microsof 365 E3 e licenças antivirus	

3.3. O objeto da contratação também está alinhado com a Estratégia de Governo Digital 2024 e em consonância com o Plano Diretor de Tecnologia da Informação (PDTI) 2024/2025 do *Conselho Regional de Contabilidade do Pará*, conforme demonstrado abaixo

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	Objetivos Estratégicos
5010	MODERNIZAÇÃO DO PARQUE DE INFORMÁTICA (HARDWARE E SOFTWARE).
12	AMPLIAR E INTEGRAR O USO DA TECNOLOGIA DA INFORMAÇÃO NO SISTEMA CFC/CRCS

O PDTI – 2024/2025, aprovado na plenária de fevereiro de 2024

3.4. Por tratar de oferta de serviços públicos digitais, o objeto da contratação será integrado à Plataforma Gov.br, nos termos do [Decreto nº 8.936, de 19 de dezembro de 2016](#), e suas atualizações, de acordo com as especificações deste Termo de Referência.

3.5. PARCELAMENTO DA SOLUÇÃO DE TIC

3.5.1. O parcelamento da solução não é viável, tendo em vista que, o contrato dispõe de apenas um item (com dois tipos) não é viável o parcelamento deste para a execução do contrato, nesse sentido, a padronização do serviço contratados é imprescindível, pois assim se evita possíveis ocorrências de incompatibilidades de suprimentos.

3.6. RESULTADOS E BENEFÍCIOS A SEREM ALCANÇADOS

3.6.1. Para que o conjunto de atividades funcione, é imprescindível a contratação deste objeto, a aquisição deste novo appliance e a contratação da licença para uso no firewall, além de substituir equipamento anterior pela falta de atualização e pelo tempo de uso, tendo por objetivo prover uma melhor configuração do acesso aos sistemas informatizados e à rede mundial de computadores, diminuindo o risco de falta de conectividade e do acesso à rede corporativa

4. REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos necessários ao atendimento da necessidade:

4.1.1. A contratação deverá obedecer a quantidade e às definições do item 2 e seus subitens deste Termo de Referência.

4.1.2. A solução deverá estar acompanhada de sua documentação técnica completa e atualizada, preferencialmente, no idioma português, falado e escrito no Brasil, compreendendo manuais, guias de instalação e outros pertinentes.

4.1.3. A documentação deverá ser fornecida em sua forma original, impressa ou em mídia digital, não sendo aceitas cópias de qualquer tipo, mesmo que autenticadas, e deverá ser disponibilizada no site do fabricante para download.

Requisitos de Negócio:

4.1.4. A presente contratação orienta-se pelos seguintes requisitos de negócio:

4.1.4.1. Console de gerenciamento centralizado;

- 4.1.4.2. Gerenciamento por grupos (integração com o Microsoft Active Directory);
- 4.1.4.3. Anti-malware/anti-vírus;
- 4.1.4.4. Anti-Ransomware;
- 4.1.4.5. IPS host;
- 4.1.4.6. IDS host;
- 4.1.4.7. Firewall host;
- 4.1.4.8. Filtro de conteúdo Web (classificação de site);
- 4.1.4.9. Suporte a Windows, iOS e Linux;
- 4.1.4.10. Proteção para solução de e-mail (Microsoft Exchange);
- 4.1.4.11. Gerenciamento de vulnerabilidades e correções;
- 4.1.4.12. Integração com soluções de SIEM;
- 4.1.4.13. Controle de dispositivos removíveis (USB);
- 4.1.4.14. Proteção proativa e instantânea contra ameaças desconhecidas;
- 4.1.4.15. Implementar técnicas de EDR (Endpoint Detection and Response).
- 4.1.4.16. As versões das licenças deverão ser as mais recentes disponibilizadas no mercado pelo fabricante.
- 4.1.4.17. As atualizações ou correções das versões das licenças serão realizadas durante todo o período de vigência contratual.
- 4.1.4.18. As soluções devem estar aderentes à infraestrutura tecnológica do CRCPA e serem compatíveis com os sistemas operacionais Microsoft Windows (64 bits), Linux e MacOS.
- 4.1.4.19. O detalhamento das especificações técnicas, encontra-se no **Anexo I(0462219)**.

4.1.4.20. **CLASSIFICAÇÃO DOS SERVIÇOS E FORMA DE SELEÇÃO DO FORNECEDOR**

4.1.4.20.1. Trata-se de serviço comum de caráter continuado sem fornecimento de mão de obra em regime de dedicação exclusiva, a ser contratado mediante dispensa licitação, **com base no Inciso II, do Art. 75 da Lei nº 14.133/2021.**

4.1.4.20.2. A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e o CRCPA, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

Requisitos de Capacitação

4.2. Considerando que se trata de uma solução para a qual a equipe de TI do CRCPA pode não ter conhecimentos técnicos suficientes para a operação, faz parte da solução a realização de treinamentos específicos.

4.2.1. Os treinamentos deverão ser presenciais tipo hands on e conduzidos por profissional qualificado pela fabricante, com ao menos uma das certificações (Certified Professional: Kaspersky EDR Foundations ou Certified Professional Kaspersky Endpoint Security and Management) da solução ofertada na proposta ou similar ao produto, com apresentação do correspondente documento de certificação, em versão original e sua validade pelo fabricante, e que seja efetivo no quadro de funcionários de empresa pertencente ao programa de parceiros oficial da fabricante, com mais de 03 (três) anos de registro em CTPS e realizados nas dependências do Conselho Regional de Contabilidade do Pará.

4.2.2. O treinamento deverá ser com a mesma base da versão dos softwares e hardwares da fabricante que serão instalados no CRCPA.

4.2.3. O material didático a ser utilizado no treinamento deverá ser disponibilizada pela empresa do fabricante e da mesma versão dos softwares e hardwares que serão instalados no CRCPA.

4.2.3.1. Todos os recursos necessários à efetiva prestação do treinamento, como: servidores, banco de dados, infraestrutura de rede de dados, entre outros, deverão ser disponibilizados pelo Cliente, uma vez

que o treinamento será na sede do Conselho Regional de Contabilidade do Pará.

4.2.3.2. O treinamento deverá ser com a mesma base da versão dos softwares e hardwares da fabricante que serão instalados no CRCPA.

4.2.3.3. O material didático a ser utilizado no treinamento deverá ser disponibilizada pela empresa do fabricante e da mesma versão dos softwares e hardwares que serão instalados no CRCPA.

4.2.3.4. Todos os recursos necessários à efetiva prestação do treinamento, como: servidores, banco de dados, infraestrutura de rede de dados, entre outros, deverão ser disponibilizados pelo Cliente, uma vez que o treinamento será na sede do Conselho Regional de Contabilidade do Pará. (Caso necessário)

4.2.3.5. Todas as despesas com transporte, hospedagem, alimentação, locação de sala de aula (se necessário) e qualquer outra que seja necessária à efetiva realização do treinamento, são de responsabilidade da Contratada.

4.2.3.6. Os treinamentos deverão ser realizados de segunda à sexta-feira, em horário comercial.

4.2.4. Serviço de Capacitação Técnica

4.2.4.1. O treinamento deve ser majoritariamente hands-on ("mão na massa"), relativo a todos os itens de hardware e software da solução de segurança;

4.2.4.2. Deve ser ministrado por profissional que detenha certificação conferida pelo fabricante como no mínimo a certificação (Certified Professional: Kaspersky EDR Foundations ou Certified Professional Kaspersky Endpoint Security and Management) da solução ofertada;

4.2.4.3. Disponibilizar documentação técnica operacional dos procedimentos de instalação da solução realizada pela CONTRATADA;

4.2.4.4. Deve permitir a participação de 02 (dois) profissionais da CONTRATANTE;

4.2.4.5. O treinamento deverá possibilitar a operação, manuseio, gerenciamento, configuração, administração e utilização dos elementos da solução ofertada conforme necessidade da CONTRATANTE;

4.2.4.6. O treinamento deverá contemplar, no mínimo os seguintes tópicos:

a) Funcionalidades básicas do antivírus: senha de administração e etc;

b) Procedimento de registro e ativação de licenças;

c) Procedimento de atualização de software;

d) Configuração de proteção endpoints (Antivírus de arquivos, de web e de e-mail, proteção de rede, detecção de comportamento, remediação, prevenção de exploits, HIPS, AMSI, anti-cryptor, prevenção de ataque BadUSB);

e) Configuração do gerenciamento de segurança (Firewall, Web, dispositivo, controles de aplicativos, Cloud Discovery);

f) Com fazer a Avaliação das vulnerabilidades, inventário de software/hardware;

g) Fazer identificação do recurso EDR (análise de causa-raiz);

h) Geração de relatórios diversos da plataforma;

i) Monitoramento do dashboard.

4.2.4.7. A capacitação deverá ter carga horária de 12 horas, em data e horário a ser definido entre as partes, podendo serem distribuídas entre a execução do treinamento e/ou do serviço;

4.2.4.8. Deverá ser fornecido pela CONTRATADA todo o material audiovisual, didático e eletrônico, preferencialmente em português, utilizado na realização do treinamento;

4.2.4.9. A CONTRATADA arcará com todas as despesas relativas aos seus profissionais e técnicos envolvidos no treinamento.

4.2.5. Serviço de Instalação e Configuração da Solução

4.2.5.1. A instalação deverá ser realizada presencialmente nas dependências do CONTRATANTE, por profissional da CONTRATADA devidamente certificado pelo fabricante do firewall, com no mínimo a certificação (Certified Professional: Kaspersky EDR Foundations ou Certified Professional Kaspersky Endpoint Security and Management) da solução ofertada;

4.2.5.2. Todo o trabalho de instalação física e conexões de cabos serão realizadas pela equipe da CONTRATADA;

4.2.5.3. Instalação de modo a garantir total interoperabilidade no ambiente de datacenter do CRCPA;

4.2.5.4. A CONTRATADA deverá cumprir com todas as exigências técnicas e funcionais relacionadas com a solução ofertada, que deve ser implantado durante o período contratado, sem ônus para a CONTRATANTE;

4.2.5.5. Configuração e ajustes em conjunto com as necessidades definidas pela Contratante para:

- a) Servidor de Administração;
- b) Instalação remota do Kaspersky e em loco;
- c) Criação de tarefas e leitura de eventos;
- d) Ajustes nos dispositivos gerenciados;
- e) Definições de Política e tarefas;
- g) Escopo de Gereação de Relatórios;

4.2.5.9. Ao concluir o serviço de instalação e configuração a CONTRATADA deverá fornecer relatório técnico detalhado (documentação), ou seja, documentação técnica operacional do procedimento da instalação da solução, informando todos os procedimentos realizados, em formato PDF.

4.3. REQUISITOS LEGAIS

4.3.1. O PRESENTE PROCESSO DE CONTRATAÇÃO DEVE ESTAR ADERENTE À [CONSTITUIÇÃO FEDERAL](#), À [LEI Nº 14.133/2021](#), À [INSTRUÇÃO NORMATIVA SGD/ME Nº 94, DE 2022](#), [INSTRUÇÃO NORMATIVA SEGES/ME Nº 65, DE 7 DE JULHO DE 2021](#), [LEI Nº 13.709, DE 14 DE AGOSTO DE 2018](#) (LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD) E A OUTRAS LEGISLAÇÕES APLICÁVEIS;

4.3.2. As soluções de TI escolhidas devem estar em conformidade com as legislações respectivas das soluções escolhidas: Assinatura da licença do Antivírus do item 2.1.

4.3.3. Lei nº 8.248, de 23 de outubro de 1991, que dispõe sobre a capacitação e competitividade do setor de informática e automação.

4.3.4. Decreto nº 7.174, de 12 de maio de 2010, que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal e faz exigência contratual de comprovação da origem dos bens importados oferecidos pelos licitantes e da quitação dos tributos de importação a eles referentes, que deve ser apresentada no momento da entrega do objeto, sob pena de rescisão contratual e multa.

4.3.5. [Instrução Normativa SLTI/MP nº 01, 19 de janeiro de 2010](#), que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal.

4.3.6. [Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022](#), que Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISF do Poder Executivo Federal;

4.3.7. Portaria SLTI/MP nº 20, de 14 de junho de 2016, que dispõe sobre orientações para contratação de soluções de Tecnologia da Informação no âmbito da Administração Pública Federal direta, autárquica e fundacional.

4.3.8. Orientação Técnica - TI Controle, nº 01 de 2010, que dispõe sobre boas práticas para a estimativa de preços na contratação de bens e serviços de TI.

4.3.9. Norma complementar nº 11/IN 01/DSIC/GSIPR, que estabelece as diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicação (SIC), nos órgãos da Administração Pública Federal.

4.3.10. [Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação](#).

4.3.11. [Resolução CRCPA n.º 470/2023](#), que aprovou o orçamento do CRCPA para o exercício de 2024.

4.3.12. Projeto 5022 do CFC, de apoio financeiro aos Conselhos Regionais de Contabilidade para atualização e ampliação do parque de informática.

4.3.13. Plano Anual de Contratações de 2024 aprovado pela [Portaria CRCPA nº 044/2023](#) de 27 de outubro de 2023.

4.3.14. [Resolução CRCPA n.º 473/2024](#) de fevereiro de 2024 que aprovou o PDTI biênio 2024/2025.

4.4. Requisitos de Suporte Técnico

4.4.1. A Contratada deverá disponibilizar suporte técnico do fabricante via *Help Desk* ou telefone e/ou *E-mail*.

4.4.2. Os serviços de suporte técnico do sistema deverão ter o prazo do contrato meses, compreendendo em;

a) Esclarecimentos de dúvidas e soluções de problemas garantir a correção dos problemas e erros detectados após a instalação sem ônus para o CRCPA.

4.5. Requisitos Temporais

4.5.1 Rotinas de Execução
· Prazos
O equipamento e software, deverão ser entregues e instalados em, no máximo 05 (cinco) dias corridos, a contar do recebimento da Ordem de Fornecimento de Bens (OFB) , emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante.
a) Customização das configurações dos equipamentos; b) Identificação dos equipamentos; (se necessário) c) Implantação dos softwares de gerenciamento; (se necessário) d) Treinamento de equipe do CRCPA;
· Horários
Dia útil, das 8h00 às 12h e das 13h00 às 17h.
· Locais de Entrega
Conselho Regional de Contabilidade do Pará, situado Av. Presidente Vargas nº 640, Campina, 5º Andar do Edifício Selecto –Cep: 66017000 - Belém-PA-
Quantidade mínima de bens ou serviços para comparação e controle
<i>Não se aplica – devido ao tipo de contratação</i>
Mecanismos Formais de Comunicação entre a Contratada e a Administração
<i>Está no item 4.9 e anexo A</i>
Forma de Pagamento em Função dos Resultados
<i>Item 8 e anexo</i>

4.6.Requisitos de Segurança e Privacidade

A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação do Contratante, e No que couber, o “Guia de Requisitos e de Obrigações quanto a Segurança da Informação e Privacidade” deverá ser observado (vide Seção 7 do Anexo da IN SGD/ME nº 94/2022. Guia disponível em: <https://www.gov.br/governodigital/pt-br/contratacoes/instrucao-normativa-sgd-me-no-94-de-23-de-dezembro-de-2022>).

Os serviços contratados deverão ser prestados em conformidade com leis, normas e diretrizes vigentes no âmbito da Administração Pública Federal, relacionadas à Segurança da Informação e Comunicações (SIC); em especial atenção ao Guia de Requisitos e de Obrigações quanto a Segurança da Informação e Privacidade” Com a finalidade de garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações e a privacidade dos dados. Guia disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_requisitos_obrigacoes.pdf.

A CONTRATADA deverá credenciar junto ao CONTRATANTE seus profissionais que venham a ser designados para prestar serviços de forma presencial, bem como aqueles autorizados a retirar e/ou entregar documentos junto ao CONTRATANTE. Assim como deverá identificar qualquer equipamento de sua propriedade que venha a ser instalado nas dependências do CONTRATANTE, utilizando placas de controle patrimonial, selos de segurança, etc. A CONTRATADA deverá comprometer-se, por si e por seus funcionários, em documento formal, a aceitar e aplicar rigorosamente todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação do CONTRATANTE – inclusive com a assinatura de TERMO de responsabilidade e manutenção de sigilo. A CONTRATADA deverá adotar critérios adequados para o processo seletivo de profissionais que irão atuar diretamente na execução do OBJETO, com o propósito de evitar a incorporação de perfis que possam comprometer a segurança ou credibilidade do CONTRATANTE.

A CONTRATADA deverá comunicar ao CONTRATANTE, com a antecedência mínima necessária, qualquer ocorrência de transferência, remanejamento ou demissão de funcionários envolvidos diretamente na execução do CONTRATO, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do CONTRATANTE porventura colocados à disposição para realização dos serviços contratados.

4.7. Requisitos Sociais, Ambientais e Culturais

Os equipamentos devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais: A contratada deverá adotar as práticas de sustentabilidade ambiental na execução do objeto, quando couber, conforme disposto no Art. 144 da Lei nº13.144/2021 e IN SLTI/MP nº 1, de 19 de janeiro de 2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional.

4.8. Requisitos de Projeto e de Implementação

Não se aplica por se tratar de um processo de contratação de 1 objeto simples e sem alteração no escopo.

4.9. Requisitos de Garantia, Manutenção e Assistência Técnica

O prazo de garantia é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), e suas atualizações.

4.9.1. A licitante deverá prover suporte técnico do fabricante necessário ao atendimento das necessidades do CRCPA e dentro do escopo solicitado, contando com tele-atendimento, via número telefônico específico. Os serviços da central de suporte deverão abranger abertura de chamados, controle de chamados em andamento, resolução de dúvidas correlatas à solução implantada.

4.9.2. O suporte técnico do fabricante deverá ser disponibilizado aos usuários, mediante a utilização dos seguintes meios de comunicação:

- a) telefone: de segunda a sexta-feira, das 08h00min às 17h;
- b) internet para a realização de consultas e abertura de chamados: 24 horas por dia, 7 dias por semana e 365 dias por ano;
- c) e-mail: para envio de solicitações e serviços: 24 horas, 7 dias por semana, 365 dias por ano.

4.10. Requisitos de Experiência Profissional

4.10.1 Será de responsabilidade da Contratada, para garantir a celeridade e a qualidade da prestação dos serviços, manter à disposição do CRCPA os profissionais em quantidade suficiente e qualificados (com experiência e capacidade técnica) para cumprimento das atividades, de acordo com o disposto neste Termo de Referência.

4.10.2. A Contratante poderá, de acordo com a qualidade do serviço prestado, solicitar a substituição de profissionais da equipe por outros que atendam aos requisitos técnicos, de formação e de experiência exigidos neste Termo de Referência.

4.10.3. A Contratada deverá formalizar a indicação de preposto da empresa e substituto eventual para a coordenação dos serviços e suporte administrativo inerente às atividades a serem executadas, garantido um serviço de alto padrão, sem nenhum custo adicional para o CRCPA.

4.10.4. O especificado no subitem 4.10.3 diz respeito a:

- a) Gerenciamento do contrato;
- b) Gerenciamento do pessoal local e remotamente;
- c) Controle das atividades desenvolvidas pelos profissionais;
- d) Gerenciamento de contingência na manutenção da execução ininterrupta dos serviços;
- e) Gerenciamento e política de segurança a ser adotada pela Contratada para garantir e manter o sigilo e a integridade das informações acessadas pelos profissionais; e
- f) Gerenciamento do conhecimento dos serviços executados para o seu repasse em caso de substituição.

4.10.5. Dificuldades ou interrupções no serviço por problemas aplicação, quando detectados pelo Conselho Regional de Contabilidade do Pará, serão comunicados à Contratada por meio de e-mail, com confirmação de recebimento do registro. A Contratada terá até 02 (duas) horas para responder à Contratante. Período superior ao descrito, caso não justificado, será considerado atraso na prestação do serviço e, a partir de então, poderá ser aplicada sanção conforme o item 7.10..

4.10.6. A Contratada deverá disponibilizar suporte técnico aos usuários dos serviços, *online* ou por telefone, de segunda a sexta-feira, por pelo menos 8 (oito) horas diárias, em horário compreendido entre 8h e 17h30, durante todo o período de vigência do contrato, com vistas à solução de eventuais problemas, falhas e dúvidas na operacionalização da aplicação. (Se houver)

4.10.7. Todas as despesas decorrentes dos serviços de manutenção do período da garantia, durante o período de vigência contratual, deverão estar incluídas no preço total do contrato. (se houver)

4.10.8. Os serviços de manutenção das aplicações, que serão executados pela empresa contratada, referem-se ao desenvolvimento das atividades de correção de eventuais falhas no funcionamento dos softwares, elucidações de dúvidas técnicas sobre suas funcionalidades e implantação de novas versões do produto, que deverão ser disponibilizadas tão logo sejam lançadas. (Caso necessário)

4.11. Requisitos de Formação da Equipe

4.11.1. A contratada deverá atender aos requisitos do item 4.10 e se responsabilizar e pelos técnicos envolvidos.

4.12. Requisitos de Metodologia de Trabalho

4.12.1. O fornecimento das licenças estão condicionado ao recebimento pelo Contratado de Ordem de fornecimento de Bens (OFB) emitida pela Contratante.

4.12.2. A OFB indicará o tipo da licença, a quantidade e a localidade na qual as licenças deverão ser entregues.

4.12.3. O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 horas por dia e 7 dias por semana de maneira eletrônica e 24 horas por dia e 6 dias por semana por via telefônica.

4.12.4. O andamento do fornecimento dos equipamentos deve ser acompanhado pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

4.12.5. Na execução das demandas a CONTRATADA deve zelar pela observância às políticas, diretrizes, procedimentos, padrões e modelos para as atividades de gestão e fiscalização de contratos e planejamento de contratações – dentre esses, destacadamente, a Metodologia de Desenvolvimento de Sistemas (MDS-MEC), a Metodologia de Gerenciamento de Projetos (MGP-MEC) o Guia de Métricas do MEC e a Política de Gerenciamento de Configuração - disponível para acesso e download através do seguinte endereço eletrônico: <http://ramec.mec.gov.br/dti-diretoria-de-tecnologia-da-informacao/contratacao-fabrica-de-software>.

4.12.6. No que couber, quando não especificado de outra forma, o processo de trabalho é aquele descrito no Modelo de Execução para cada ITEM de serviço, conforme detalhado nos requisitos específicos no item 2.1 do TR. Também, no que couber, na execução dos serviços a CONTRATADA deve manter observância às políticas, regulamentações, especificações técnicas e orientações definidos pelos seguintes padrões de GOVERNO:

a) Padrões de Interoperabilidade de Governo Eletrônico (e-PING) e Modelo de Acessibilidade em Governo Eletrônico (e-MAG), conforme as Portarias Normativas SLTI nº 5, de 14 de julho de 2005 e nº 3, de 7 de maio de 2007 e suas atualizações;

b) Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), conforme a Medida Provisória nº 2.200-2, de 24 de agosto de 2001, e suas atualizações, quando houver necessidade de utilização de certificação digital; e

c) Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ Brasil), quando a solução abranger a gestão de documentos arquivísticos digitais e não digitais, conforme Resolução do CONARQ nº 32, de 17 de maio de 2010 e suas atualizações. Ainda, nos termos do Decreto nº 8.936, de 19 de dezembro de 2016, e do inc. III do art. 6º da Instrução Normativa SGD/ME nº 94/2022, as demandas que produzirem software/sistema que se consubstancie em serviço público digital devem ser integradas à Plataforma de Cidadania Digital.

A metodologia aplicada no trabalho contratado será ágil, visando a realização de **melhorias e alterações constantes**, baseadas no feedback dos usuários, dos próprios clientes e até do time interno de suporte.

4.13. Indicação de marcas ou modelos

4.13.1. Na presente contratação será admitida a indicação da(s) seguinte(s) marca(s), característica(s) ou modelo(s), de acordo com as justificativas contidas nos Estudos Técnicos Preliminares no item 2.1.2, em decorrência da necessidade de manter a compatibilidade com plataformas e padrões já adotados pela Administração, conforme [Art. 41 da Lei nº 14.133/2021](#).

4.14. Subcontratação

4.14.1. Não é admitida a subcontratação do objeto contratual.

4.15. Garantia da Contratação

4.15.1. Não será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual e condições descritas nas cláusulas do contrato.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

- 5.1.1. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;
- 5.1.2. encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;
- 5.1.3. receber o objeto fornecido pelo Contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
- 5.1.4. aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;
- 5.1.5. liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;
- 5.1.6. comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;
- 5.1.7. definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do Contratado, com base em pesquisas de mercado, quando aplicável;
- 5.1.8. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer;
- 5.1.9. É de responsabilidade do CRCPA o fornecimento de pontos de rede, energia elétrica, mobiliário e espaço físico para a instalação dos equipamentos, objeto deste Edital;
- 5.1.10. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;
- 5.1.11. Disponibilizar técnico da T.I. para a instalação/atualização de drivers nos equipamentos dos usuários;
- 5.1.12. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;
- 5.1.13. Permitir o acesso e a permanência dos profissionais técnicos da CONTRATADA em suas dependências, devidamente identificados e uniformizados para a execução de serviços correlatos ao objeto deste Edital, apenas;
- 5.1.14. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;
- 5.1.15. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;
- 5.1.16. Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas neste Termo de Referência;
- 5.1.17. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da contratada, no que couber, em conformidade com o item 7.6 do Anexo XI da IN SEGES/MP n. 5/2017, alterada pela a

5.2. São obrigações do CONTRATADO:

5.2.1. Prestar os serviços, o objeto deste Procedimento, de acordo com os prazos de entrega e de instalação dos equipamentos e assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

5.2.1.1. Somente será considerado cumprido o prazo de instalação quando os equipamentos estiverem em condições de atender às especificações de operação para as quais tenha sido contratado;

5.2.1.2. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência acompanhado da respectiva nota fiscal; Nota Explicativa: As indicações referentes ao objeto deverão ser aquelas exigidas no edital. A garantia da qualidade (ou prazo de validade) do objeto deve guardar conformidade com o prazo de garantia ou validade exigido no edital ou com aquele ofertado pelo licitante na proposta, se for o caso.

5.2.2. Responsabilizar-se pelos vícios e danos decorrentes do objeto; (Se houver)

5.2.3. A empresa deverá garantir a correção de erros que forem detectados após a implantação sem ônus para o CRCPA;

5.2.4. Comunicar ao CRCPA, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

5.2.5. Apresentar a relação dos equipamentos entregues, fazendo constar marca, modelo, tipo do equipamento e outras informações relevantes para inventário ou auditoria; (Se houver)

5.2.6. Responsabilizar-se pelo transporte dos equipamentos, independentemente da distância da sede da CONTRATADA e sem ônus para a CRCPA, quando da remoção, instalação, reinstalação ou desmobilização, parcial ou total, correlatos à execução dos serviços objeto deste contrato; (Se houver)

5.2.7. Havendo a necessidade de contratação de empresa transportadora, os custos dos serviços decorrentes dessa contratação correrão por conta da CONTRATADA; (Se houver)

5.2.8. Prestar os serviços rigorosamente de acordo com as especificações da respectiva proposta, obedecendo as disposições legais e regulamentos pertinentes;

5.2.9. A CONTRATADA não poderá instalar, desinstalar, remanejar ou remover qualquer equipamento ou recursos sem prévia autorização do CRCPA;

5.2.10. Arcar com os custos de instalação inicial, remoção final e remoções/instalações decorrentes de necessidades de ações preventivas, corretivas e/ou otimização do parque instalado;

5.2.11. Realizar as remoções ou intervenções nos equipamentos somente por técnicos qualificados e credenciados da CONTRATADA e seguindo normas e orientações do fabricante;

5.2.12. Todas e quaisquer ações a serem executadas nos equipamentos deverão ocorrer por conta da CONTRATADA, mediante prévio aviso ao CRCPA;

5.2.13. Atender prontamente quaisquer exigências do Fiscal do Contrato inerentes ao objeto do futuro contrato;

5.2.14. Apresentar, após o fornecimento do serviço, a fatura/nota fiscal, que somente será encaminhada para pagamento após o aceite definitivo dos itens pelo fiscal do contrato;

5.2.15. Observar as disposições e especificações contidas neste Termo de Referência, devendo atendê-las em sua plenitude;

5.2.16. Comunicar ao CRCPA, por escrito, qualquer anormalidade de caráter urgente e prestar os esclarecimentos julgados necessários.;

5.2.17. Manter, durante toda a execução do futuro contrato, em compatibilidade com as obrigações e serem assumidas, todas as condições de qualificação, exigidas neste Termo de Referência, devendo

comunicar à Contratante a superveniência de fato impeditivo da manutenção dessas condições;

5.2.18. Reparar quaisquer danos diretamente causados à Contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela Contratante.;

5.2.19. Apresentar, quando da entrega do objeto, os manuais básicos de instruções de uso e de recursos de operação dos equipamentos, escritos em língua portuguesa;

5.2.20. Propiciar todos os meios e facilidades necessárias à fiscalização da Solução de Tecnologia da Informação pela Contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária;

5.2.21. Quando especificada, manter, durante a execução do Contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da Solução de Tecnologia da Informação.;

5.2.22. Deverá disponibilizar e orientar sobre o acesso aos treinamentos online disponibilizados pela Kaspersky sem custos adicional para o CONTRATANTE;

5.2.23. Diante de situações de irregularidades de caráter urgente deverá comunicar, por escrito, ao CRCPA com os esclarecimentos julgados necessários e, as informações sobre possíveis paralisações de serviços, a apresentação de relatório técnico ou razões justificadoras a serem apreciada se decididas pelo agente designado;

5.2.24. Manter equipamentos e sistemas em perfeitas condições de funcionamento e qualidade durante toda a execução do contrato;

5.2.25. Prestar todas as informações e esclarecimentos à CONTRATANTE, inclusive de ordem financeira, julgados necessários à boa execução do contrato;

5.2.26. Manter seus profissionais identificados com crachás e uniformes nas dependências do CRCPA, como também garantir que, durante a execução dos serviços, os ambientes sejam mantidos em perfeitas condições de higiene e de segurança;

5.2.27. A inadimplência da CONTRATADA, com referência aos encargos estabelecidos em lei ou neste Termo de Referência, não transfere a responsabilidade por seu pagamento à CONTRATANTE, nem pode onerar o objeto deste contrato, razão pela qual a CONTRATADA renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com a CONTRATANTE;

5.2.29. Transferir conhecimento a, no mínimo, 2 (dois) servidores/colaboradores designados pelo CRCPA, relativo ao uso e operação dos recursos disponíveis pelos equipamentos, de forma que sejam utilizados da forma correta e integralmente;

5.2.30. Comunicar ao Departamento de Tecnologia da Informação do CRCPA, por escrito, qualquer anormalidade de caráter urgente e prestar os esclarecimentos julgados necessários;

5.2.31. Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, uma vez que os seus empregados não manterão nenhum vínculo empregatício com o CRCPA;

5.2.32. Todos os encargos de possível demanda trabalhista, civil ou penal, relacionada à execução do contrato, originariamente ou vinculada por prevenção, conexão ou continência; Os encargos fiscais e comerciais resultantes desta contratação;

5.2.33. A inadimplência da CONTRATADA, com referência aos encargos estabelecidos em lei ou neste Termo de Referência, não transfere a responsabilidade por seu pagamento à CONTRATANTE, nem pode onerar o objeto deste contrato, razão pela qual a CONTRATADA renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com a CONTRATANTE;

5.2.34. Aceitar, durante a vigência do Contrato, nas mesmas condições contratuais com os acréscimos ou supressões do objeto, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato, durante a sua vigência (Art.125 Da Lei nº 14.133/21);

5.2.35. Fornecer, na assinatura do contrato endereço de correspondência, telefone, e-mail e procedimentos para encaminhamento do Ofício por parte do CRCPA;

5.2.36. Manter seu endereço de correspondência e telefone atualizado durante toda a vigência do contrato;

5.2.37. Responder, em no máximo 48 horas corridas, quaisquer questionamentos realizados pelo CRCPA.

5.2.38. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

5.2.39. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da Contratante;

5.2.40. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação;

a) Indicar formalmente e por escrito, no prazo máximo de 02 dias úteis após a assinatura do contrato, junto à contratante, um preposto idôneo com poderes de decisão para representar a contratada, principalmente no tocante à eficiência e agilidade da execução do objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato;

b) Executar o objeto do contrato em estreita observância dos ditames estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

c) Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato, sem prévia autorização da contratante;

d) Não fazer uso das informações prestadas pela contratante para fins diversos do estrito e absoluto cumprimento do contrato em questão;

e) Outras obrigações que se apliquem, de acordo com o objeto da contratação, observando, no que couber, as “Ações de Responsabilidade da Contratada”, constantes no “Guia de Requisitos e de Obrigações quanto a Segurança da Informação e Privacidade”. Guia disponível em : <https://www.gov.br/governodigital/pt-br/governanca-dados/GuiaRequisitosdeSIparaContratacoesdeTI.pdf>.

5.3. DA ALTERAÇÃO SUBJETIVA

5.3.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

6 – MODELO DE EXECUÇÃO DO CONTRATO

Rotinas de Execução

Do Encaminhamento Formal de Demandas

6.1. O gestor do contrato emitirá a Ordem de fornecimento de bens (OFB) para a entrega dos bens desejados.

6.2. O Contratado deverá fornecer as licenças com as mesmas configurações e quantidades definidas na OFB.

6.3. O detalhamento está descrita no item 4.5 deste TR.

6.2. Quantidade mínima de bens ou serviços para comparação e controle (Caso necessário)

6.2.1. A quantidade está especificada e detalhada no item 2.3 e seus subitens neste TR.

Formas de transferência de conhecimento

6.3. O repasse de instruções e orientações técnicas referentes a solução contratada, deverão ser realizadas observando-se o que se segue:

6.3.1. Deve ser fornecido treinamento técnico-operacional tipo hands on e presencial, para 2 (dois) empregados do CRCPA, que cubram, preferencialmente em português e, alternativamente, em inglês:

a) a configuração e gerenciamento da solução;

b) técnicas de análise de erros e detecção de falhas de configuração, *debug* e *troubleshooting*;

c) configuração e operação dos subsistemas de prevenção de intrusão (IPS) e filtro de conteúdo.

6.3.2. Deve ser fornecido treinamento para 2 (dois) empregados do CRCPA, de no mínimo, 24 (vinte e quatro) horas de duração.

6.4. Requisitos da Capacitação

6.4.1. Os treinamentos deverão ser presenciais tipo hands on e conduzidos por profissional qualificado pela fabricante, com ao menos umas das certificações (Certified Professional: Kaspersky EDR Foundations ou Certified Professional Kaspersky Endpoint Security and Management) da solução ofertada, que seja efetivo no quadro de funcionários de empresa pertencente ao programa de parceiros oficial da fabricante, com vínculo empregatício e registro em CTPS com data anterior do publicação do edital. A capacitação deverá ocorrer nas dependências do Conselho Regional de Contabilidade do Pará.

6.4.1.1. A exigência da certificação do profissional é necessária para garantir a qualidade do treinamento e expertise para que, o profissional possua conhecimento da ferramenta do objeto do treinamento.

6.4.1.2. O treinamento deverá ser com a mesma base da versão dos softwares e hardwares da fabricante que serão instalados no CRCPA.

6.4.1.3. O material didático a ser utilizado no treinamento deverá ser disponibilizada pela empresa do fabricante e da mesma versão dos softwares e hardwares que serão instalados no CRCPA.

6.4.1.4. Todos os recursos necessários à efetiva prestação do treinamento, como: servidores, banco de dados, infraestrutura de rede de dados, entre outros, deverão ser disponibilizados pelo Cliente, uma vez que o treinamento será na sede do Conselho Regional de Contabilidade do Pará.

6.4.1.5. Todas as despesas com transporte, hospedagem, alimentação, locação de sala de aula (se necessário) e qualquer outra que seja necessária à efetiva realização do treinamento, são de responsabilidade da Contratada.

6.4.1.6. Os treinamentos deverão ser realizados de segunda à sexta-feira, em horário comercial.

6.4.1.7. O **Serviço de Capacitação Técnica**

6.4.2. Os itens do Serviço de Capacitação Técnica e Serviço de Instalação e Configuração da Solução estão descritos nos itens 4.2.4. e 4.2.5. respectivamente.

Procedimentos de transição e finalização do contrato

6.5. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

Quantidade mínima de bens ou serviços para comparação e controle

6.6. Cada OFB conterà a quantidade a ser fornecida, incluindo a sua localização e o prazo, conforme definições deste TR.

6.7. A quantidade está especificada e detalhada no item 2.3 e seus subitens neste TR.

6.8. Mecanismos formais de comunicação

6.8.1. São definidos como mecanismos formais de Comunicação, entre a Contratante e o Contratado, os seguintes:

6.8.2. A ORDEM DE SERVIÇO (OS) é o instrumento normativo padrão para formalização das demandas à CONTRATADA. A critério do CONTRATANTE, esse instrumento poderá ser substituído por registros eletrônicos em sistema informatizado hábil – inclusive no que diz respeito ao registro de requisições de serviço. Encaminhadas as demandas à CONTRATADA, mediante ORDENS DE SERVIÇO, a ciência do PREPOSTO (e/ou do LÍDER TÉCNICO do item de serviço) deve ser registrada em até, no máximo, 01:00 (uma) hora útil após recebimento do documento, na forma hábil pactuada entre as partes (inclusive por intermédio de sistema informatizado). Decorrido esse prazo e não firmada a ciência espontânea, o CONTRATANTE considerará a ORDEM DE SERVIÇO do Anexo A como recebida pela CONTRATADA.

6.8.3. As ORDENS DE SERVIÇOS conterão, no mínimo, as seguintes informações, podendo ser enviados por e-mails e via whats app:

- a) Numeração de identificação (ID);
- b) Título e descrição da solicitação;
- c) Identificação do responsável pela demanda na área requisitante (Fiscal Requisitante);
- d) Identificação do Gestor do Contrato;
- e) Especificações quanto ao tipo e ao volume da demanda (incluindo descrição de macro-atividades a serem executadas, quando aplicável);
- f) Especificação quanto a prazos de execução;
- g) Expectativa de remuneração, quando for o caso; e
- h) Outras informações necessárias, quando for o caso.

6.8.4. Os prazos específicos, quando não fixados no modelo de execução ou nos requisitos específicos do ITEM DE SERVIÇO, serão consignados na respectiva ORDEM DE SERVIÇO. Como padrão e quando não especificado em contrário, todos os prazos serão considerados horas corridas e/ou dias úteis – conforme o caso.

6.8.5. As ORDENS DE SERVIÇO serão numeradas sequencialmente a partir da primeira ordem emitida acompanhada com o ano correspondente ao de sua abertura. Ao início de um novo ano, a numeração da OS poderá ser reiniciada. As Ordens de Serviços poderão ser abertas e gerenciadas por meio de sistema informatizado. Um modelo genérico de ORDEM DE SERVIÇO é apresentado no ANEXO A, sendo que, a critério do CONTRATANTE, este modelo poderá ser alterado a qualquer tempo para atender às necessidades do serviço – devendo manter as informações mínimas necessárias à sua correta execução.

6.8.6. A abertura de ORDENS DE SERVIÇO observará a capacidade de gestão do CONTRATANTE para gerenciar projetos e acompanhar demandas. Assim, como poderão ser replanejadas a qualquer momento a critério do CONTRATANTE, considerando suas necessidades e prioridades, o que será registrado no Histórico de Ocorrências.

6.8.7. É importante ressaltar que as Ordens Serviço emitidas serão mecanismos de avaliação para pagamento do serviço prestado pela CONTRATADA, sendo necessário cumprir, pois haverá um Instrumento de Medição de Resultado (IMR) - Anexo C, para esta avaliação.

6.9. Manutenção de Sigilo e Normas de Segurança

6.9.1. A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

6.9.2. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se nos ANEXO B.

7. MODELO DE GESTÃO DO CONTRATO

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

7.3. As comunicações entre o órgão ou entidade e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

7.5. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput) , nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

7.5.1. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

7.5.2. O fiscal técnico do contrato anotarà no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

7.5.3. Identificada qualquer inexecução ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

7.5.4. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

7.5.5. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprezadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato.

7.5.6. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

7.5.7. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação do contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

7.5.8. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

Reunião Inicial

7.5. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução do contrato.

7.6. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da [IN SGD/ME nº 94](#),

[de 2022](#), e ocorrerá em até 02(*dois*) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

7.7. A pauta desta reunião observará, pelo menos:

7.7.1. Presença do representante legal da contratada, que apresentará o seu preposto;

7.7.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

7.7.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

7.7.4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

7.7.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

7.8. Controle e Fiscalização da Execução

7.8.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos ([Lei nº 14.133, de 2021, art. 117, caput](#)), nos termos do art. 33 da [IN SGD nº 94, de 2022](#), observando-se, em especial, as rotinas a seguir.

7.9. Fiscalização Técnica

7.9.1. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da [IN SGD nº 94, de 2022](#), acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. ([Decreto nº 11.246, de 2022, art. 22, VI](#));

7.9.1.1. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. ([Lei nº 14.133, de 2021, art. 117, §1º](#), e [Decreto nº 11.246, de 2022, art. 22, II](#));[A1]

7.9.1.2. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. ([Decreto nº 11.246, de 2022, art. 22, III](#));

7.9.1.3. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. ([Decreto nº 11.246, de 2022, art. 22, IV](#)).

7.9.1.4. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprezadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. ([Decreto nº 11.246, de 2022, art. 22, V](#)).

7.9.1.5. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual ([Decreto nº 11.246, de 2022, art. 22, VII](#)).

7.10. Fiscal Administrativo

7.10.1. O fiscal administrativo do contrato, além de exercer as atribuições previstas no [art. 33, IV, da IN SGD nº 94, de 2022](#), verificará a manutenção das condições de habilitação do Contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário ([Art. 23, I e II, do Decreto nº 11.246, de 2022](#)).

7.10.1.1. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as

providências cabíveis, quando ultrapassar a sua competência; ([Decreto nº 11.246, de 2022, art. 23, IV](#)).

7.11. Gestor do Contrato

7.11.1. O gestor do contrato, além de exercer as atribuições previstas no [art. 33, I, da IN SGD nº 94, de 2022](#), coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. ([Decreto nº 11.246, de 2022, art. 21, IV](#)).

7.12. O gestor do contrato acompanhará a manutenção das condições de habilitação do Contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. ([Decreto nº 11.246, de 2022, art. 21, III](#)).

7.13. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. ([Decreto nº 11.246, de 2022, art. 21, II](#)).

7.14. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. ([Decreto nº 11.246, de 2022, art. 21, VIII](#)).

7.5. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o [art. 158 da Lei nº 14.133, de 2021](#), ou pelo agente ou pelo setor com competência para tal, conforme o caso. ([Decreto nº 11.246, de 2022, art. 21, X](#)).

7.6. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual. ([Decreto nº 11.246, de 2022, art. 22, VII](#)).

7.7. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. ([Decreto nº 11.246, de 2022, art. 21, VI](#)).

7.8. Critérios de Aceitação (Caso necessário)

7.8.1. A avaliação da qualidade dos produtos entregues, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:

7.8.2. Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não reconicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos end-of-life).

7.8.3. Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, frisagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos não previstos nas especificações técnicas ou, ainda, com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes que sejam fisicamente ou logicamente incompatíveis.

7.8.4. Todos os componentes internos do(s) equipamento(s) deverá(ão) estar instalado(s) de forma organizada e livres de pressões ocasionados por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado.

7.8.5. O número de série de cada equipamento deve ser obrigatório e único, afixado em local visível, na parte externa do gabinete e na embalagem que o contém. Esse número deverá ser identificado pelo fabricante, como válido para o produto entregue e para as condições do mercado brasileiro no que se refere à garantia e assistência técnica no Brasil.

7.8.6. Serão recusados os produtos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos.

7.8.7. Os produtos, considerando a marca e modelo apresentados na licitação, não poderão estar fora de linha comercial, considerando a data de LICITAÇÃO (abertura das propostas). Os produtos devem ser fornecidos completos e prontos para a utilização, com todos os acessórios, componentes, cabos etc.

7.8.8. Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização do Contratante, em modo definitivo (licenças perpétuas), legalizado, não sendo admitidas versões "shareware" ou "trial". O modelo do produto ofertado pelo licitante deverá estar em fase de produção pelo fabricante (no Brasil ou no exterior), sem previsão de encerramento de produção, até a data de entrega da proposta.

7.8.9. A Contratante poderá optar por avaliar a qualidade de todos os equipamentos fornecidos ou uma amostra dos equipamentos, atentando para a inclusão nos autos do processo administrativo de todos os documentos que evidenciem a realização dos testes de aceitação em cada equipamento selecionado, para posterior rastreabilidade.

7.8.10. Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao Contratante o direito de não receber o OBJETO cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no CONTRATO. Quando for o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.

7.8.11. Durante a vigência do contrato o CRCPA adotará o Instrumento de Medição de Resultado (IMR) - Anexo C - de acordo com os parâmetros estabelecidos na IN SEGES/MPDG n.º 94/2022.

7.8.11.1. O IMR é o mecanismo que define, em bases compreensíveis, tangíveis, objetivamente observáveis e comprováveis, os níveis esperados de qualidade da prestação do serviço e respectivas adequações de pagamento;

7.8.11.2. A forma de medição do serviço e pagamento à Contratada será por Acordo de Níveis de Serviços. Os indicadores mínimos de desempenho para aferição da qualidade esperada da prestação dos serviços constam do Anexo C deste Termo de Referência.

7.8.11.3. Mensalmente, a fiscalização do contrato deverá verificar o nível de atendimento aos indicadores previstos no IMR. (Se necessário)

7.8.11.4. Em caso de não cumprimento das metas estabelecidas, o fiscal efetuará as glosas na medição dos serviços, conforme demonstrativo Anexo E e o entregará à Contratada para emissão da Nota Fiscal, com os devidos descontos. (Se necessário).

7.9. Procedimentos de Teste e Inspeção

7.9.1. Não se aplica neste contrato, pois não terá desenvolvimento de sistemas.

7.10. Níveis Mínimos de Serviço Exigidos

7.10.1. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pelo Contratante para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

IAE – INDICADOR DE ATRASO NO FORNECIMENTO DO EQUIPAMENTO

Tópico	Descrição
Finalidade	<i>Medir o tempo de atraso na entrega dos produtos e serviços constantes na Ordem de Fornecimento de Bens.</i>
Meta a cumprir	IAE < = 0 <i>A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Fornecimento de Bens dentro do prazo previsto.</i>
Instrumento de medição	<i>OFB, Termo de Recebimento Provisório (TRP)</i>
Forma de acompanhamento	<i>A avaliação será feita conforme linha de base do cronograma registrada na OFB. Será subtraída a data de entrega dos produtos da OFB (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OFB.</i>
Periodicidade	<i>Para cada Ordem de Fornecimento de Bens encerrada e com Termo de Recebimento Definitivo.</i>
Mecanismo de Cálculo (métrica)	<p>IAE = <u>TEX – TEST</u></p> <p>Onde:</p> <p>IAE – Indicador de Atraso de Entrega da OFB;</p> <p>TEX – Tempo de Execução – corresponde ao período de execução da OFB, da sua data de início até a data de entrega dos produtos da OFB.</p> <p>A data de início será aquela constante na OFB; caso não esteja explícita, será o primeiro dia útil após a emissão da OFB.</p> <p>A data de entrega da OFB deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OFB continua a correr, findando-se apenas quando o Contratado entrega os produtos da OFB e haja aceitação por parte do fiscal técnico.</p> <p>TEST – Tempo Estimado para a execução da OFB – constante na OFB, conforme estipulado no Termo de Referência.</p>
Observações	<p><i>Obs1: Serão utilizados dias corridos na medição.</i></p> <p><i>Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.</i></p>
Início de Vigência	<i>A partir da emissão da OFB.</i>
Faixas de ajuste no pagamento e Sanções	<p><i>Para valores do indicador IAE:</i></p> <p><i>Menor ou igual a 0 – Pagamento integral da OFB;</i></p> <p><i>De 1 a 60 - aplicar-se-á glosa de 0,1666% por dia de atraso sobre o valor da OFB ou fração em atraso.</i></p> <p><i>Acima de 60 - aplicar-se-á glosa de 10% bem como multa de 2% sobre o valor OFB ou fração em atraso.</i></p>

7.11. Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

A finalidade das sanções administrativas em licitações e contratos é reprovar a conduta praticada pelo sancionado, desestimular a sua reincidência, bem como prevenir sua prática futura pelos demais licitantes e contratados. As sanções podem ter caráter preventivo, educativo, repressivo ou visar à reparação de danos pelos responsáveis que causem prejuízos ao erário público. Trata-se, portanto, de um poder-dever da ADMINISTRAÇÃO que deve atuar visando impedir ou minimizar os danos causados pelos licitantes e contratados que descumprem suas obrigações.

7.11.1. Comete infração administrativa nos termos do Art. 156 combinado com os Art. 157 e 158 da Lei nº 14.133, de 2021, a Contratada que:

7.11.1.1. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

7.11.1.2. ensejar o retardamento da execução do objeto;

7.11.1.3. falhar ou fraudar na execução do contrato;

7.11.1.4. comportar-se de modo inidôneo;

7.11.1.5. cometer fraude fiscal;

7.11.2. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

7.11.2.1. Advertência, por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;

7.11.3. Na hipótese da contratada não entregar o objeto contratado no prazo estabelecido, caracterizar-se-á atraso, e será aplicada multa de 0,5% (zero vírgula cinco por cento) por dia, até o máximo de 30% (trinta por cento) sobre o valor da contratação;

7.11.4. O contratante a partir do 10º (décimo) dia de atraso poderá recusar o objeto contratado, ocasião na qual será cobrado a multa relativa à recusa e não mais diária por atraso, ante a inacumulabilidade da cobrança.

7.11.5. Em caso de recusa do objeto contratado aplicar-se-á multa de 10% (dez por cento) sobre o valor da contratação.

7.11.5.1 Entende-se configurada a recusa, além do descumprimento do prazo estabelecido no item 4.5.1 deste Termo e Referência, as hipóteses em que a contratada não apresentar situação regular conforme exigências contidas no edital, neste Termo de Referência e no contrato.

7.11.6. Caso a contratada não atenda aos demais prazos e obrigações constantes no edital, neste Termo de Referência e no instrumento contratual, aplicar-se-á multa de 0,2% (zero virgula dois por cento) por dia, limitada a 10% (dez por cento) sobre o valor da contratação.

7.11.7. A multa aplicada em razão de atraso injustificada não impede que a administração rescinda a contratação e aplique outras sanções prevista em lei.

7.11.8 Multa por Rescisão.

7.11.8.1 Nas hipóteses unilateral, deve ser aplicada multa de 10% (dez por cento) sobre o valor da contratação.

7.11.8.2 Não deve haver cumulação entre a multa prevista neste artigo e a multa específica prevista para outra inexecução que enseje em rescisão. Nessa hipótese, deve ser aplicada a multa de maior valor.

7.11.8.3 As multas descritas serão descontadas de pagamentos a serem efetuados ou de garantia, quando houver, ou ainda cobradas administrativamente e, na impossibilidade, judicialmente.

7.11.9. suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

7.11.9.1. impedimento de licitar e contratar com órgãos e entidades da União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

7.11.9.2. A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 7.5.1 deste Termo de Referência.

7.11.10. declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

7.11.11. As sanções e glosas do CRCPA previstas nos subitens definidas na tabela abaixo das ocorrências de 1 à 13 poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

7.11.12. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

7.11.13. As penalidades serão obrigatoriamente registradas no SICAF.

7.11.14. As sanções e glosas do CRCPA poderão ser utilizadas, devendo-se observar a definição clara e detalhada das sanções administrativas, considerando:

- a) vinculação aos termos contratuais;
- b) proporcionalidade das sanções previstas ao grau do prejuízo causado pelo descumprimento das respectivas obrigações;
- c) as situações em que advertências serão aplicadas;
- d) as situações em que as multas serão aplicadas, com seus percentuais correspondentes, que obedecerão a uma escala gradual para as sanções recorrentes;
- e) as situações em que o contrato será rescindido por parte da Administração devido ao não atendimento de termos contratuais, da recorrência de aplicação de multas ou outros motivos;
- f) as situações em que a contratada terá suspensa a participação em licitações e impedimento para contratar com a Administração; e
- g) as situações em que a contratada será declarada inidônea para licitar ou contratar com a Administração, conforme previsto em Lei.

Observar a Legislação que trata de proteção de dados pessoais (Lei nº 13.709, de 2018) e proteção do consumidor (Lei nº 8.078, de 11 de setembro de 1990), no que couber.

Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela Contratante, conforme a tabela abaixo:

Id	Ocorrência	Glosa / Sanção
1	Não comparecer injustificadamente à Reunião Inicial.	Advertência. Em caso de reincidência, 5% sobre o valor total do Contrato.

2	Quando convocado dentro do prazo de validade da sua proposta, não celebrar o Contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não manter a proposta, falhar ou fraudar na execução do Contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.	A Contratada ficará impedida de licitar e contratar com a União, Estados, Distrito Federal e Municípios e, será descredenciada no SICAF, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da Lei nº 10.520/2002, pelo prazo de até 5 (cinco) anos, sem prejuízo das demais cominações legais, e multa de 5% do valor da contratação.
3	Ter praticado atos ilícitos visando frustrar os objetivos da licitação.	A Contratada será declarada inidônea para licitar e contratar com a Administração.
4	Demonstrar não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
5	Não executar total ou parcialmente os serviços previstos no objeto da contratação.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
6	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por até de 30 dias, sem comunicação formal ao gestor do Contrato.	Multa de 5% sobre o valor total do Contrato. Em caso de reincidência, configura-se inexecução total do Contrato por parte da empresa, ensejando a rescisão contratual unilateral.
7	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por mais de 30 (trinta) dias, sem comunicação formal ao gestor do contrato.	Contratada será declarada inidônea para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
8	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 48 horas úteis.	Multa de 5% sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela Contratante, até o limite de 15 dias úteis.
		Após o limite de 2 dias úteis, aplicar-se-á multa de 5% do valor total do Contrato.
9	Provocar intencionalmente a indisponibilidade da prestação dos serviços quanto aos componentes de software (sistemas, portais, funcionalidades, banco de dados, programas, relatórios, consultas, etc).	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.

10	Permitir intencionalmente o funcionamento dos sistemas de modo adverso ao especificado na fase de levantamento de requisitos e às cláusulas contratuais, provocando prejuízo aos usuários dos serviços.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
11	Comprometer intencionalmente a integridade, disponibilidade ou confiabilidade e autenticidade das bases de dados dos sistemas.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
12	Comprometer intencionalmente o sigilo das informações armazenadas nos sistemas da contratante.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
13	Não atender ao indicador de nível de serviço IAE (Indicador de Atraso de Entrega de OS)	<p>Glosa de 0,2% sobre o valor da OS para valores do indicador IAE de 0,11 a 0,20.</p> <p>Glosa de 0,3% sobre o valor da OS para valores do indicador IAE de 0,21 a 0,30.</p> <p>Glosa de 0,4% sobre o valor da OS para valores do indicador IAE de 0,31 a 0,50.</p> <p>Glosa de 0,5% sobre o valor da OS para valores do indicador IAE de 0,51 a 1,00.</p> <p>Multa de 5% sobre o valor do Contrato e Glosa de 1% sobre o valor da OS, para valores do indicador IAE maiores que 1,00.</p>

7.11.15. Nos termos do [art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022](#), será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que p Contratado:

7.11.16 não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

7.11.17. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada

8. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento do Objeto

8.1. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e

fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

8.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 5 (*cinco*) dias, a contar da notificação do Contratado, às suas custas, sem prejuízo da aplicação das penalidades.

8.3. O recebimento definitivo ocorrerá no prazo de 10 (dez) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

8.4. Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o [inciso II do art. 75 da Lei nº 14.133, de 2021](#), o prazo máximo para o recebimento definitivo será de até 05 (cinco) dias úteis.

8.5. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

8.6. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do [art. 143 da Lei nº 14.133, de 2021](#), comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

8.7. O prazo para a solução, pelo Contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

8.8. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

Liquidação

8.9. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do [art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022](#).

8.9.1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o [inciso II do art. 75 da Lei nº 14.133, de 2021](#).

8.10. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

8.10.1. o prazo de validade;

8.10.2. a data da emissão;

8.10.3. os dados do contrato e do órgão Contratante;

8.10.4. o período respectivo de execução do contrato;

8.10.5. o valor a pagar; e

8.10.6. eventual destaque do valor de retenções tributárias cabíveis.

8.11. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante;

8.12. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta *on-line* ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no [art. 68 da Lei nº 14.133, de 2021](#).

8.13. A Administração deverá realizar consulta ao SICAF para:

- a) verificar a manutenção das condições de habilitação exigidas no edital;
- b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

8.14. Constatando-se, junto ao SICAF, a situação de irregularidade do Contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do Contratante.

8.15. Não havendo regularização ou sendo a defesa considerada improcedente, o Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do Contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

8.16. Persistindo a irregularidade, o Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao Contratado a ampla defesa.

8.17. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o Contratado não regularize sua situação junto ao SICAF.

Prazo de pagamento

8.18. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da [Instrução Normativa SEGES/ME nº 77, de 2022](#).

8.19. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice *a ICTI e ou IPCA* de correção monetária.

Forma de pagamento

8.20. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.

8.21. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

8.22. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

8.23. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

8.24. O Contratado regularmente optante pelo Simples Nacional, nos termos da [Lei Complementar nº 123, de 2006](#), não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

9. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

Forma de seleção e critério de julgamento da proposta

9.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO ou DISPENSA, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo *menor preço*.

9.2. O regime da execução dos contratos é empreitada por preço global, pois a **contratação e a execução do serviço é por preço certo e total**, e o tipo e critério de julgamento da licitação é o menor preço para a seleção da proposta mais vantajosa, utilizado para compras e serviços de modo geral e para contratação de bens e serviços de informática.

Da Aplicação da Margem de Preferência

9.3. Não será aplicada margem de preferência na presente contratação

Exigências de habilitação

9.4. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

9.4.1. *Previamente à celebração do contrato, a Administração verificará o eventual descumprimento das condições para contratação, especialmente quanto à existência de sanção que a impeça, mediante a consulta a cadastros informativos oficiais, tais como:*

a) SICAF;

b) *Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (www.portaldatransparencia.gov.br/ceis);*

c) *Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/cnep>)*

9.4.2. *A consulta aos cadastros será realizada em nome da empresa interessada e de seu sócio majoritário, por força do artigo 12 da Lei nº 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.*

9.4.3. *Caso conste na Consulta de Situação do interessado a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.*

9.4.4. *A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.*

9.4.5. *O interessado será convocado para manifestação previamente a uma eventual negativa de contratação.*

9.4.6. *Caso atendidas as condições para contratação, a habilitação do interessado será verificada por meio do SICAF, nos documentos por ele abrangidos.*

9.4.7. *É dever do interessado manter atualizada a respectiva documentação constante do SICAF, ou encaminhar, quando solicitado pela Administração, a respectiva documentação atualizada.*

9.4.8. *Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.*

9.4.9. *Se o interessado for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, caso exigidos, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.*

9.4.10. *Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.*

9.4.11. *Para fins de habilitação, deverá o interessado comprovar os seguintes requisitos, que serão*

exigidos conforme sua natureza jurídica:

Habilitação jurídica

9.5. **Pessoa física:** cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

9.6. **Empresário individual:** inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

9.7. **Microempreendedor Individual - MEI:** Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

9.8. **Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI:** inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

9.9. **Sociedade empresária estrangeira:** portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução [Normativa DREI/ME n.º 77, de 18 de março de 2020](#).

9.10. **Sociedade simples:** inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

9.11. **Filial, sucursal ou agência de sociedade simples ou empresária:** inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

9.12. **Sociedade cooperativa:** ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o [art. 107 da Lei nº 5.764, de 16 de dezembro 1971](#).

9.13. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

9.14. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

9.15. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

9.16. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

9.17. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do [Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943](#);

9.18. Prova de inscrição no cadastro de contribuintes *Estadual* ou *Municipal* relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.19. Prova de regularidade com a Fazenda *Estadual* ou *Municipal/Distrital* do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

9.20. Caso o fornecedor seja considerado isento dos tributos *Estadual ou Municipal* relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

9.21. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na [Lei Complementar n. 123, de 2006](#), estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal. Ou seja, aos itens de valor correspondente a até R\$ 80.000,00 deve ser garantida a participação exclusiva de Microempresa e Empresa de Pequeno Porte (ME e EPP), conforme artigo 48, inciso I, da Lei Complementar nº 123, de 14 de dezembro de 2006, e artigo 6º do Decreto nº 8.538, de 06 de outubro de 2015).

9.22. Fornecer a Declaração de que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7º, XXXIII, da Constituição”.

Qualificação Econômico-Financeiro

9.23.1. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

9.23.2. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

9.23.3. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

9.23.3.1. Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

9.23.3.2. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura; e

9.23.3.3. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

9.23.3.4. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped. [\[MR1\]](#)

9.23.4. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

9.23.5. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor

Qualificação Técnica

9.24. Atender o item 6.4.1.

10. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

10.1. O custo estimado total da contratação é de R\$ 20.149,50 (vinte mil e cento e quarenta e nove reais e cinquenta centavos), conforme custos unitários apostos no ETP.

11. ADEQUAÇÃO ORÇAMENTÁRIA

11.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral do CRCPA.

11.2. Na forma do art. 21 da Instrução Normativa nº 94/2022, a adequação orçamentária e o cronograma

físico-financeiro contêm a estimativa do impacto econômico-financeiro no orçamento do órgão ou entidade, com indicação das fontes de recurso e o cronograma de execução física e financeira, contendo o detalhamento das etapas ou fases da Solução a ser contratada, com os principais serviços ou bens que a compõe, e a previsão de desembolso para cada uma delas:

11.3. A contratação será atendida pela seguinte dotação.

ORÇAMENTO DETALHADO				
PROJETO: 5010 - MODERNIZAÇÃO DO PARQUE DE INFORMÁTICA (HARDWARE E SOFTWARE)				
CONTA CONTÁBIL- 6.3.2.1.05.01.002 -SOFTWARES				
PROGRAMA DO PLANO DE TRABALHO: 5 - SUPORTE E APOIO A ATIVIDADES FINIS				
ITEM	CONTA	EXERCÍCIO	ESTIMATIVA	ANUAL ESTIMATIVA
1	6.3.2.1.05.01.002	2024 (JAN-DEZ)	R\$ 20.149,50	R\$ 20.149,50
ESTIMATIVA CALCULADA EM: Contrato de licenças por 36 meses para uso no antivírus, sendo paga de uma vez.				

12. DA VIGÊNCIA DO CONTRATO

12.1. O contrato vigorará por 12 (doze) meses, podendo ser prorrogável para até 10 anos, na forma dos artigos [106 e 107 da Lei nº 14.133, de 2021](#) por interesse das partes.

12.1.1. A prorrogação do contrato dependerá da verificação da manutenção da necessidade, economicidade e oportunidade da contratação, acompanhada de a realização de pesquisa de mercado que demonstre a vantajosidade dos preços contratados para a Administração.

12.1.2. O CRCPA tem a necessidade de **contratar empresa especializada na** aquisição das licenças de uso da solução de segurança antivírus Kaspersky Next EDR Foundations para estações de trabalho (endpoints), servidores e dispositivos móveis, gerenciados por solução centralizada no modelo on-premise, contemplando o serviço de implantação, com repasse de instrução e orientação técnica referente a manutenção preventiva, além da garantia, suporte técnico do fabricante e atualizações por 36 (trinta e seis) meses., para 65 usuários 5 servidores, uma vez que esta solução é necessária para o bom funcionamento das atividades e suas constantes atualizações e implementações tecnológicas.

12.1.3. A contratação tem caráter continuado sem fornecimento de mão de obra em regime de dedicação exclusiva, a ser contratada mediante Licitação do tipo **dispensa licitação, com base no Inciso II, do Art. 75 da Lei nº 14.133/21**, e será realizada em lote único com o objetivo de permitir a compatibilidade e disponibilidade dos serviços ofertados para que possam funcionar de maneira íntegra e segura.

12.1.4. Esta contratação se enquadra na definição da **IN nº 05/2017 alterada pela IN nº 49/2022, conforme preconiza o Art. 15** *“Os serviços prestados de forma contínua são aqueles que, pela sua essencialidade, visam atender à necessidade pública de forma permanente e contínua, por mais de um exercício financeiro, assegurando a integridade do patrimônio público ou o funcionamento das atividades finalísticas do órgão ou entidade, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional.”*.

12.1.5. A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração Contratante, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

12.2 PRAZO PREVISTO PARA O INÍCIO DE EXECUÇÃO DO SERVIÇO OU ENTREGA DO OBJETO

12.2.1 Os serviços deverão estar disponíveis para utilização a partir da assinatura o contrato, podendo entregar a licenças em até 05 dias atendendo o TR.

13. DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 121, de 03 de junho de 2024.

Conforme o §6º do art. 12 da IN SGD/ME nº 94, de 2022, o Termo de Referência ou Projeto Básico será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC, e aprovado pela autoridade competente.

_____ Luciano Coutinho Almeida Coord. do Setor de TI Matrícula: 0019	_____ Newton da Silva Junior Analista de TI Matrícula: 0029	_____ Gabriela Ramos dos Reis Assessora Técnica Matrícula: 0186
--	---	---

Autoridade Máxima da Área de TIC
_____ Ewerton Ribeiro Jorge Vice-Presidente de Administração

A justificativa apresentada, específicos técnicas e quantitativas, contidas no presente instrumento, demonstram-se satisfatórias e suficientes para o atendimento às necessidades do CRCPA.

Autoridade Competente
_____ Ailton Ramos Corrêa Júnior Presidente do CRCPA

*Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União - CNMLC
Atualização: maio/2023*

Termo de Referência Aquisição de Bens de TIC - Licitação

Elaborado pela Secretaria de Gestão. Complementado e Uniformizado pela CNMLC

Identidade visual pela Secretaria de Gestão

Por fim, sugiro que o processo siga o rito do processo, para à contratação do serviço.



Documento assinado eletronicamente por **Luciano Coutinho Almeida, Analista - Sistemas / Desenvolvimento**, em 23/08/2024, às 12:12, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Newton da Silva Junior, Analista - Sistemas / Desenvolvimento**, em 27/08/2024, às 09:30, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Gabriela Ramos dos Reis, Assessora**, em 29/08/2024, às 16:30, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Ailton Ramos Côrrea Junior, Presidente**, em 29/08/2024, às 19:09, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Ewerton Ribeiro Jorge, Vice-Presidente**, em 30/08/2024, às 14:30, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0468847** e o código CRC **EDCE9C95**.



CONSELHO REGIONAL DE CONTABILIDADE DO PARÁ

Rua Avertano Rocha, 392, - Bairro Comércio, Belém/PA, CEP 66023-120 Telefone: (91) 3202-4150 - www.crcpa.org.br

E-mail: crcpa@crcpa.org.br

Processo n.º : 9079612110000416.000012/2024-81

ANEXO I

ESPECIFICAÇÕES DO OBJETO

A solução de software de segurança e os serviços oferecidos devem atender aos seguintes requisitos técnicos:

Especificações técnicas da solução para ambiente Windows, Linux e Mobile.

1. Requisitos Gerais:

1.1. O console de gerenciamento deve ser on premise, fornecido como um appliance virtual ou executável para instalação em servidores Windows.

1.1.1. Para o caso de appliance virtual, deverá suportar no mínimo o Hypervisor VMWare vSphere 6.7 ou superior;

1.1.2. Para o caso de instalação em sistema operacional Windows, deverá ser compatível, no mínimo, com a versão Microsoft Windows Server 2008R2 ou superior.

1.2. Toda e qualquer licença de banco de dados necessária para o completo funcionamento da solução (todas as funcionalidades ativas) deverá ser fornecida pela CONTRATADA;

1.3. A solução deverá permitir a inclusão de um módulo de balanceamento para casos em que vários servidores tenham a mesma função (para alta disponibilidade, recuperação de desastres, performance, dentre outras necessidades);

1.4. A solução deve possuir console de gerenciamento centralizado com acesso via WEB (HTTPS) ou MMC (Microsoft Management Console);

1.5. O console de gerenciamento deve ser único e capaz de gerenciar todos os dispositivos (endpoints, servidores e dispositivos móveis);

1.6. O Console de Gerenciamento deve conter:

1.6.1. Painel para monitoramento;

1.6.2. Capacidade de criação de relatórios e envio automático dos mesmos (via e-mail);

1.6.3. Mecanismo para envio de notificações administrativas (via e-mail);

1.7. Deve permitir Inventário da Rede.

1.8. A console central deve mostrar quantos dispositivos estão sendo gerenciados, assim como informações sobre cada um deles, como dados sobre o Agente e Endpoint instalados, Sistema Operacional, IP etc.

1.9. Todos os softwares, módulos e plugins pertencentes à solução de segurança deverão ser administrados pela mesma console de gerenciamento.

1.10. Deve possuir a capacidade de autenticação dos usuários da console de gerenciamento através do Microsoft Active Directory.

1.10.1. Deve permitir a definição de perfis com diferentes níveis de privilégios de administração da solução, baseados em usuários ou grupos do Microsoft Active Directory.

1.11. Deve permitir o bloqueio das configurações dos softwares da solução (Agente e Endpoint) instalado nas estações e servidores, de maneira que o usuário não consiga alterá-las.

1.11.1. A solução de segurança deve ter a capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web, a serem escolhidas pelo administrador da solução.

1.12. Capacidade de instalar remotamente a solução de antivírus nas estações (endpoints) e servidores Windows, através de compartilhamento administrativo, login script e GPO do Microsoft Active Directory, no mínimo.

1.13. Capacidade de gerar pacotes customizados (auto-executáveis) para a instalação do software, contendo todas as informações necessárias para o funcionamento do produto (licenças, configurações, etc).

1.14. Capacidade de importar a estrutura do Microsoft Active Directory para a descoberta de máquinas da rede corporativa.

1.15. Capacidade de monitorar a rede, em diferentes subredes, a fim de encontrar máquinas novas, para a instalação automática da solução de segurança.

1.16. Deve ser capaz de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem a necessidade de instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar o tráfego da rede.

1.17. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar o tráfego de link entre sites diferentes.

1.18. Deve permitir a herança de tarefas e políticas na estrutura de hierarquia de servidores administrativos.

1.19. Capacidade de conectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

a) Mudança de gateway;

b) Mudança de subnet;

c) Mudança de domínio;

d) Mudança de servidor DHCP;

e) Mudança de servidor DNS.

1.20. Deve permitir que dispositivos gerenciados se conectem via Internet ao servidor de gerência, caso estejam fora da rede corporativa, sem a necessidade de utilização de recursos “em nuvem”.

1.21. Capacidade de realizar atualização incremental de vacinas nos computadores clientes a partir da rede local e da Internet.

1.22. A atualização incremental de vacinas deve ser disponibilizada, no mínimo, com frequência diária.

1.23. A solução deve possuir integração com o Active Directory, de maneira a permitir a definição de políticas diferentes, baseadas em usuários ou grupos.

1.24. A solução deve possuir a capacidade de geração de um pacote de instalação pré-configurado com base nas políticas corporativas, para a distribuição para dispositivos móveis.

1.25.

2. Do módulo de proteção de endpoint

2.12. A solução proposta deverá proteger os sistemas operacionais abaixo:

2.12.1. Windows 7

2.12.2. Windows 8

2.12.3. Windows 8.1

2.12.4. Windows 10

2.12.5. Windows 11

2.13. Servidores

2.13.1. Windows Small Business Server 2011

2.13.2. Windows MultiPoint Server 2011

2.13.3. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

2.14. Servidores de terminal Microsoft

2.14.1. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

2.15. Sistemas operacionais Linux de 32 bits (Disponível somente a partir de 300 Licenças através do Expert View):

2.15.1. CentOS 6.7 e posterior

2.15.2. Debian GNU/Linux 11.0 e posterior

2.15.3. Debian GNU/Linux 12.0 e posterior

2.15.4. Red Hat Enterprise Linux 6.7 e posterior

2.16. Sistemas operacionais Linux de 64 bits (Disponível somente a partir de 300 Licenças através do Expert View):

2.16.1. Amazon Linux 2.

2.16.2. CentOS 6.7 e mais tarde

2.16.3. CentOS 7.2 e posterior.

2.16.4. CentOS Stream 8.

2.16.5. CentOS Stream 9.

2.16.6. Debian GNU/Linux 11.0 e posterior.

2.16.7. Debian GNU/Linux 12.0 e posterior.

2.16.8. Linux Mint 20.3 e superior.

2.16.9. Linux Mint 21.1 e posterior.

2.16.10. openSUSE Leap 15.0 e posterior.

2.16.11. Oracle Linux 7.3 e posterior.

2.16.12. Oracle Linux 8.0 e posterior.

- 2.16.13. Oracle Linux 9.0 e posterior.
- 2.16.14. Red Hat Enterprise Linux 6.7 e posterior
- 2.16.15. Red Hat Enterprise Linux 7.2 e posterior.
- 2.16.16. Red Hat Enterprise Linux 8.0 e posterior.
- 2.16.17. Red Hat Enterprise Linux 9.0 e posterior.
- 2.16.18. Rocky Linux 8.5 e posterior.
- 2.16.19. Rocky Linux 9.1.
- 2.16.20. SUSE Linux Enterprise Server 12.5 ou posterior.
- 2.16.21. SUSE Linux Enterprise Server 15 ou posterior.
- 2.16.22. Ubuntu 20.04 LTS.
- 2.16.23. Ubuntu 22.04 LTS.
- 2.16.24. Sistemas operacionais Arm de 64 bits:
- 2.16.25. CentOS Stream 9.
- 2.16.26. SUSE Linux Enterprise Server 15.
- 2.16.27. Ubuntu 22.04 LTS.
- 2.17. Sistemas operacionais MAC OS:
- 2.17.1. macOS 12 – 14
- 2.18. Ferramentas de virtualização MAC OS:
- 2.18.1. Parallels Desktop 16 para Mac Business Edition
- 2.18.2. VMware Fusion 11.5 Professional
- 2.18.3. VMware Fusion 12 Professional
- 2.19. A solução proposta deverá suportar as seguintes plataformas virtuais:(Disponível somente a partir de 300 Licenças através do Expert View)
- 2.19.1. VMware Workstation 17.0.2 Pro
- 2.19.2. VMware ESXi 8.0 Update 2
- 2.19.3. Microsoft Hyper-V Server 2019
- 2.19.4. Citrix Virtual Apps e Desktop 7 2308
- 2.19.5. Citrix Provisioning 2308
- 2.19.6. Citrix Hypervisor 8.2 Update 1

3. Do módulo de gerenciamento avançado (Disponível somente a partir de 300 Licenças através do Expert View)

- 3.12. A solução proposta deve suportar arquitetura cloud-native e on-premise;
- 3.13. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:
 - 3.13.1. Amazon Web Services
 - 3.13.2. Microsoft Azure
- 3.14. A solução proposta deve incluir as seguintes opções de integração SIEM:
 - 3.14.1. HP (Microfoco) ArcSight
 - 3.14.2. IBM QRadar

3.14.3. Splunk

3.14.4. Kaspersky KUMA

3.15. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

3.16. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;

3.17. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

3.18. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

3.19. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

3.20. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

3.21. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.

3.22. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

3.23. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.

3.24. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

3.25. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em um único/múltiplos dispositivos com base nas seguintes regras de ativação:

3.25.1. Status do dispositivo

3.25.2. Tag

3.25.3. Diretório ativo

3.25.4. Proprietários de dispositivos

3.25.5. Hardware

3.26. A solução proposta deve suportar os seguintes canais de entrega de notificação:

3.26.1. E-mail

3.26.2. Registro de sistema

3.26.3. SMS

3.27. A solução proposta deve ter a capacidade de etiquetar/marcas computadores com base em:

3.27.1. Atributos de rede

3.27.2. Nome

3.27.3. Domínio e/ou Sufixo de Domínio

3.27.4. Endereço de IP

3.27.5. Endereço IP para servidor de gerenciamento

3.27.6. Localização no Active Directory

3.27.7. Unidade organizacional

3.27.8. Grupo

3.27.9. Sistema operacional

3.27.10. Número do pacote de serviço

3.27.11. Arquitetura Virtual

3.27.12. Registro de aplicativos

3.27.13. Nome da Aplicação

3.27.14. Versão do aplicativo

3.27.15. Fabricante

3.27.16. Tipo e versão

3.27.17. Arquitetura

3.28. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

3.29. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

3.30. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

3.30.1. Dispositivos Desktop/Servidores

3.30.2. Dispositivos móveis

3.30.3. Dispositivos de rede

3.30.4. Dispositivos virtuais

3.30.5. Componentes OEM

3.30.6. Periféricos de computador

3.30.7. Dispositivos IoT conectados

3.30.8. Telefones VoIP

3.30.9. Repositórios de rede

3.31. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

3.31.1. Nome da Aplicação

3.31.2. Caminho do aplicativo

3.31.3. Metadados do aplicativo

3.31.4. Aplicativo Certificado digital

3.31.5. Categorias de aplicativos predefinidas pelo fornecedor

3.31.6. SHA256 e MD5

3.32. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

3.32.1. Bluetooth

3.32.2. Dispositivos móveis

3.32.3. Modems externos

3.32.4. CD/DVD

3.32.5. Câmeras e scanners

3.32.6. MTPs

3.32.7. E a transferência de dados para dispositivos móveis

3.33. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

3.34. A solução sugerida deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

3.35. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

3.35.1. Estruturas de domínios e grupos de trabalho do Windows

3.35.2. Estruturas de grupos do Active Directory

3.35.3. Conteúdo de um arquivo de texto criado manualmente pelo administrador

3.36. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.

3.37. A solução proposta deve permitir realizar as seguintes ações para endpoints:

3.37.1. Verificação manual;

3.37.2. Verificação no acesso;

3.37.3. Verificação por demanda;

3.37.4. Verificação de arquivos compactados

3.37.5. Verificação de arquivos individuais, pastas e unidades;

3.37.6. Bloqueio e verificação de scripts

3.37.7. Proteção contra alteração de registros;

3.37.8. Proteção contra estouro de buffer;

3.37.9. Verificação em segundo plano/inativa

3.38. Verificação de unidade removível na conexão com o sistema;

3.39. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.

3.40. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.

3.41. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.

3.42. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.

3.43. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.

3.44. A solução proposta deve suportar Windows Failover Cluster.

3.45. A solução proposta deve ter um recurso de clustering integrado.

3.46. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.

3.47. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as

restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.

3.48.O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.

3.49. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.

3.50.A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.

3.51. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.

3.52. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.

3.53.A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.

3.54.A solução proposta deverá possuir controles para download de DLL e drivers.

3.55.A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo específico de prevenção de intrusão.

3.56.A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.

3.57.A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).

3.58.A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.

3.59.A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.

3.60.A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.

3.61.A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.

3.62.A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.

3.63.A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança antimalware através do servidor de administração.

3.64.A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.

3.65.A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações antimalware instalados, e para distribuir notificações sobre eventos por e-mail.

3.66.A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou

em computadores selecionados.

3.67.A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.

3.68.A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal. .

3.69.A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.

3.70.A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.

3.71.A solução proposta deve permitir ao administrador personalizar relatórios.

3.72.A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.

3.73.A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.

3.74.A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.

3.75.A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.

3.76.A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.

3.77.A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.

3.78.O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;

3.79.O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.

3.80. A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:

3.81. Windows

3.82. Linux

4. A solução proposta deverá suportar os seguintes servidores de banco de dados:

4.12. Windows:

4.12.1. Microsoft SQL Server

4.12.2. Microsoft Banco de dados SQL do Azure

4.12.3. MySQL Standard e Enterprise

4.12.4. MariaDB

4.12.5. PostgreSQL

4.13. Linux:

4.13.1. MySQL

4.13.2. MariaDB

4.13.3. PostgreSQL

5. A solução proposta deverá suportar as seguintes plataformas virtuais:

5.12. Windows:

5.12.1. VMware vSphere 6.7 e 7.0

5.12.2. Estação de trabalho VMware 16 Pro

5.12.3. Servidor Microsoft Hyper-V 2012 de 64 bits

5.12.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits

5.12.5. Microsoft Servidor Hyper -V 2016 de 64 bits

5.12.6. Servidor Microsoft Hyper-V 2019 de 64 bits

5.12.7. Servidor Microsoft Hyper-V 2022 de 64 bits

5.12.8. Citrix XenServer 7.1 LTSR

5.12.9. Citrix XenServer 8.x

5.12.10. Oracle VM VirtualBox 6.x

5.13. Linux:

5.13.1. VMware vSphere 6.7, 7.0 e 8.0

5.13.2. VMware Desktop 16 Pro e 17 Pro

5.13.3. Servidor Microsoft Hyper-V 2012 de 64 bits

5.13.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits

5.13.5. Microsoft Servidor Hyper -V 2016 de 64 bits

5.13.6. Servidor Microsoft Hyper-V 2019 de 64 bits

5.13.7. Servidor Microsoft Hyper-V 2022 de 64 bits

5.13.8. Citrix XenServer 7.1 e 8.x

5.13.9. Oracle VM VirtualBox 6.x e 7.x

6. Do módulo de gerenciamento simplificado (Disponível somente a partir de 300 Licenças através do Expert View):

6.1. A solução proposta deve suportar arquitetura cloud;

6.2. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

6.3. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

6.4. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.

6.5. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.

- 6.6. A solução proposta deve atender as condições apontadas no item e subítemes 6.
- 6.7. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.
- 6.8. A solução proposta deve incluir informações do endpoint:
 - 6.8.1. IP público de internet;
 - 6.8.2. IP interno do dispositivo;
 - 6.8.3. Versão do agente de proteção;
 - 6.8.4. Última comunicação com a console, contendo data e hora;
 - 6.8.5. Informações do sistemas operacional;

7. Requisitos gerais

- 7.1. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:
 - 7.1.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.
- 7.2. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
- 7.3. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).
- 7.4. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.
- 7.5. A solução proposta deve suportar o subsistema Linux no Windows.
- 7.6. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:
 - 7.6.1. Proteção contra ameaças sem arquivos (Fileless);
 - 7.6.2. Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;
- 7.7. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;
- 7.8. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.
- 7.9. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.
- 7.10. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.
- 7.11. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.
- 7.12. A solução proposta deve fornecer análise comportamental baseada em machine learning.
- 7.13. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux (Disponível somente a partir de 300 Licenças através do Expert View), através de seu console de gerenciamento.
- 7.14. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:
 - 7.14.1. Controles de aplicativos,
 - 7.14.2. Controle web e dispositivos

7.14.3. HIPS e Firewall

7.14.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;

7.15.A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.

7.16.A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.

7.17.A solução proposta deve ter bancos de dados de reputação locais e globais.

7.18.A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.

7.19. A solução proposta deve incluir um módulo capaz, no mínimo, de:

7.19.1. Bloqueio de aplicativos com base em sua categorização.

7.19.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.

7.19.3. A adição de sub-redes e a modificação de permissões de atividade.

7.20.A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.

7.21. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.

7.22. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.

7.23. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.

7.24. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.

7.25. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.

7.26. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.

7.27. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.

7.28.A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.

7.29.A solução proposta deve ser capaz de decifrar e verificar o tráfego de rede transmitido por conexões criptografadas.

7.30.A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;

7.31.A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;

7.32.A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.

7.33.A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.

7.34.A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.

7.35.A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.

7.36.A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.

7.37.A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.

7.38.A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.

7.39.A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.

7.40.A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.

7.41.A solução proposta deve ter categoria de detecção para bloquear banners de sites.

7.42.A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;

7.43.A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.

7.44.A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.

7.45.A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.

7.46.A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;

7.47.A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.

7.48.A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.

7.49.A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.

7.50.O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.

7.51.O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.

7.52.A solução proposta deve suportar o controle de scripts executados em PowerShell.

7.53.A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.

7.54. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.

7.55. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.

7.56.A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.

7.57.A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.

7.58.A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.

7.59.A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:

7.59.1. Filtro de anexos.

7.59.2. Verificação de mensagens de email ao receber, ler e enviar.

7.60.A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.

7.61.A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;

7.62.A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);

7.63.A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registro do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.

7.64.A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.

7.65.A solução proposta deve incluir suporte ao protocolo IPv6.

7.66.A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.

7.67.A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:

7.68.Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.

7.69.Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.

7.70.A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.

7.71.A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.

7.72.A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.

7.73.A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.

7.74.A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.

7.75.A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.

7.76.A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.

7.77.A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia , bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.

7.78.A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.

7.79.A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.

7.80.A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.

7.81.A solução proposta deve suportar endereços IPv6.

7.82.A solução proposta deve suportar verificação em duas etapas (autenticação).

7.83.A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.

7.84.A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.

7.85.A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.

7.86.A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.

7.87.A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.

7.88.A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.

7.89. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.

7.90. A solução proposta deve permitir a gestão de um componente que controle o trabalho com dispositivos de E/S externos.

7.91. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.

7.92. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.

7.93. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.

7.94. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.

7.95. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.

7.96. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.

7.97. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.

7.98. A solução proposta deve ter a capacidade de excluir atualizações baixadas.

7.99. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.

7.100. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.

7.101. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.

7.102. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.

7.103. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.

7.104. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.

7.105. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.

7.106. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.

7.107. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:

7.107.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.

7.107.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

7.108. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.

7.109. A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.

8. Do modulo de gerenciamento de dispositivos móveis

8.1. O modulo deve ser integrado a console de gerenciamento;

8.2. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

8.3.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)

8.4. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

8.4.1. iOS 10–17 ou iPadOS 13–17

8.5. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.

8.6. A solução proposta deve suportar dispositivos iOS supervisionados.

8.7. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.

8.8. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.

8.9. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.

8.10. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com

jogos de azar ou categorias de redes sociais).

8.11. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.

8.12. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

8.13. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.

8.14. A solução proposta deve ter recursos de containerização para dispositivos Android.

8.15. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:

8.15.1. Dados em contêineres

8.15.2. Contas de e-mail corporativo

8.15.3. Configurações para conexão à rede Wi-Fi corporativa e VPN

8.15.4. Nome do ponto de acesso (APN)

8.15.5. Perfil do Android for Work

8.15.6. Recipiente KNOX

8.15.7. Chave do gerenciador de licença KNOX

8.16. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:

8.16.1. Todos os perfis de configuração instalados

8.16.2. Todos os perfis de provisionamento

8.16.3. O perfil iOS MDM

8.17. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas

8.18. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo .

8.19. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controle de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:

8.19.1. Critérios de verificação do dispositivo;

8.19.2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;

8.20. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.

8.21. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:

8.21.1. Cartões de memória e outras unidades removíveis

8.21.2. Câmera do dispositivo

8.21.3. Conexões Wi-Fi

8.21.4. Conexões Bluetooth

8.21.5. Porta de conexão infravermelha

- 8.21.6. Ativação do ponto de acesso Wi-Fi
- 8.21.7. Conexão de área de trabalho remota
- 8.21.8. Sincronização de área de trabalho
- 8.21.9. Definir configurações da caixa de correio do Exchange
- 8.21.10. Configurar caixa de e-mail em dispositivos iOS MDM
- 8.21.11. Configure contêineres Samsung KNOX.
- 8.21.12. Definir as configurações do perfil do Android for Work
- 8.21.13. Configurar e-mail/calendário/contatos
- 8.21.14. Defina as configurações de restrição de conteúdo de mídia.
- 8.21.15. Definir configurações de proxy no dispositivo móvel
- 8.21.16. Configurar certificados e SCEP
- 8.22. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay .
- 8.23. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:
 - 8.23.1. Google Play, Huawei App Gallery e Apple App Store
 - 8.23.2. Portal de inscrição móvel KNOX
 - 8.23.3. Pacotes de instalação pré-configurados independentes
- 8.24. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.
- 8.25. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.
- 8.26. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:
 - 8.26.1. VMware AirWatch 9.3 ou posterior
 - 8.26.2. MobileIron 10.0 ou posterior
 - 8.26.3. IBM MaaS360 10.68 ou posterior
 - 8.26.4. Microsoft Intune 1908 ou posterior
 - 8.26.5. SOTI MobiControl 14.1.4 (1693) ou posterior
- 8.27. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.
- 8.28. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:
 - 8.28.1. Google Play
 - 8.28.2. Galeria de aplicativos Huawei
 - 8.28.3. Loja de aplicativos da Apple
- 8.29. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.
- 8.30. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.
- 8.31. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.
- 8.32. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.

8.33. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.

8.34. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.

8.35. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.

8.36. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.

8.37. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.

8.38. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.

8.39. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.

8.40. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.

8.41. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;

8.42. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

9. Do módulo de EDR

9.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos, conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

9.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.

9.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;

9.4. Deve apresentar as seguintes informações:

9.5.1. Processo;

9.5.2. Arquivos;

9.5.3. Chaves de registros;

9.5.4. Conexões de rede;

9.5.5. SHA256 e MD5;

9.6. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;

9.7. Deve apresentar informações detalhadas contendo:

9.7.1. Usuário que executou a ação;

9.7.2. Informações acesso privilegiado;

10. Requisitos para documentação da solução.

10.1. A documentação da solução do anti-malware incluindo ferramentas de administração, deve incluir os seguintes documentos:

10.2. Ajuda on-line para administradores

10.3. Ajuda on-line para melhores práticas de implementação

10.4. Ajuda on-line para proteção de servidores de administração

10.5. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.

10.6. Deve estar disponível página com informações de ciclo de vida das soluções e módulos.

11. Implantação e configuração da solução de segurança antivírus Kaspersky, desde o servidor de console de gerenciamento, até as estações de trabalho e servidores:

11.1. Fornecer serviço de implantação e configuração inicial da solução de software de segurança contratada.

11.2. A implantação da solução de segurança deverá ser presencial, realizada na infraestrutura do datacenter localizado na sede do CONTRATANTE.

11.2.1. A critério exclusivo da CONTRATANTE a implantação poderá ser realizada remotamente;

11.3. Programar os procedimentos de implantação e repasse de conhecimento, devendo observar as seguintes fases:

11.3.1. Planejamento do ambiente e validação dos parâmetros e requisitos técnicos;

11.3.2. Planejamento da estratégia de distribuição da solução de segurança para as máquinas clientes;

11.3.3. Instalação e configuração da Interface de Gerenciamento Centralizado, bem como em um grupo de amostragem das estações clientes;

11.3.4. Validação e testes do novo ambiente e realização de ajustes conforme a necessidade;

11.3.5. Acompanhamento do ambiente após a conclusão da instalação, até que este ambiente esteja apto à plena entrada em produção;

11.3.6. Apresentação da documentação técnica do ambiente.

11.4. A implantação da solução de segurança deverá ser realizada por profissional certificado pelo fabricante da solução ofertada na proposta, com apresentação do correspondente documento de certificação, em versão original ou cópia autenticada.

11.5. A instalação e configuração dos componentes da solução de segurança deverão ocorrer nas datas e horários definidos pela equipe técnica do CONTRATANTE, que supervisionará os trabalhos.

11.6. A solução deverá ter a capacidade de remoção do atual antivírus instalado e ser capaz de instalar de forma remota o agente do antivírus pela console de gerenciamento, e caso não tenha a capacidade de realização da remoção completa, a CONTRATADA deverá remover a atual solução utilizando scripts, softwares de terceiros, ou mesmo de forma manual, e prover a instalação da nova solução de segurança;

11.7. Atividades que exijam a paralisação ou que causem o comprometimento de serviços de informática em produção deverão ser executados fora do horário de expediente e deverão ser agendados e aprovados pela CONTRATANTE.

11.8. Deverá ser gerado um relatório pela CONTRATADA comprovando a instalação e configuração da solução, sendo que deverá estar em pleno funcionamento local e integrada ao console de gerenciamento.

11.9. Deve haver o repasse de conhecimento hands-on com relação às configurações realizadas

Luciano Coutinho Almeida
Coord. do TI/CRCPA



Documento assinado eletronicamente por **Luciano Coutinho Almeida, Analista - Sistemas / Desenvolvimento**, em 16/08/2024, às 12:56, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0462219** e o código CRC **432AE3E1**.

Referência: Processo nº 9079612110000416.000012/2024-81

SEI nº 0462219



CONSELHO REGIONAL DE CONTABILIDADE DO PARÁ
ESTUDO TÉCNICO PRELIMINAR

Processo nº 9079612110000416.000012/2024-81

Processo nº 9079612110000416.000012/2024-81

INTRODUÇÃO

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

Referência: Art. 11 da IN SGD/ME nº 94/2022.

1 – DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

1.1. Aquisição das licenças de uso da solução de segurança antivírus Kaspersky Endpoint Security para estações de trabalho (endpoints), servidores e dispositivos móveis, gerenciados por solução centralizada no modelo on-premise, contemplando o serviço de implantação, o repasse de conhecimento a manutenção preventiva/hands-on, corretiva periódica, além da garantia, suporte técnico e atualizações por 36 (trinta e seis) meses, de acordo com especificações e quantidades estabelecidas no Termo de Referência e disposições contidas na legislação vigente. É importante ressaltar atual que a licença atual irá vencer no dia 09 de setembro de 2024.

1.2. Considerando a evolução e o uso da tecnologia em todos os momentos, incluído os todos os processos deste Regional, as ameaças as ameaças e as técnicas utilizadas nos ataques cibernéticos podem comprometer arquivos, sistemas e o parque computacional do CRCPA, contaminando os dados ao ponto de acabar com todo trabalho desenvolvido pelos funcionários, além da captura dos dados, causando indisponibilidade e gerando um impacto negativo à confiabilidade dos sistemas, bem como à integridade dos dados armazenados nos computadores e dos servidores de rede da Instituição.

1.3. Diante desse contexto, a solução de antivírus do CRCPA visa a manutenção da integridade, da disponibilidade e da confiabilidade dos dados, essencial para o cumprimento das atividades do CRCPA.

1.4. Promover o atendimento aos Objetivos Estratégicos: ampliar e integrar o uso da Tecnologia da Informação do Sistema CFC/CRCs; garantir a qualidade e confiabilidade nos processos e nos procedimentos; inovar, integrar e otimizar a gestão do Sistema CFC/CRCs; assegurar adequada infraestrutura e suporte logístico às necessidades do Sistema CFC/CRCs;

1.5. Considerando ser este um recurso indispensável para a proteção dos dispositivos da Instituição, este processo tem como objetivo realizar a renovação das licenças, a fim de viabilizar a continuidade do nível de segurança e a preservação dos dados do CRCPA, contra eventuais ações de softwares maliciosos (vírus, worms, trojans, ransomware, spywares, entre outros).

1.6. Portanto, esta contratação visa garantir que esta entidade utilize de recursos tecnológicos necessários que favoreçam com a continuidade e com o aperfeiçoamento dos serviços dispensados aos setores e internos, à sociedade e aos profissionais da classe contábil.

Identificação das necessidades tecnológicas

1.7. Com a contratação, espera-se manter a segurança da rede de informática dos computadores e aprimorar com as novas versões do sistema e pacotes de segurança, garantir a melhoria contínua da infraestrutura de TI do CRCPA. Adequar a infraestrutura de TI do CRCPA, garantindo a segurança, o desempenho e o acesso aos serviços, conforme os padrões definidos.

Assegurar a qualidade dos serviços prestados e das soluções de TI fornecidas. Com intuito de entregar aos usuários finais, maior confiabilidade, credibilidade e robustez. O Conselho Regional de Contabilidade do Pará (CRCPA), continuamente, busca manter seus equipamentos de informática atualizados visando aprimorar e agilizar o trabalho de seu corpo funcional e dos que dependem de utilizar os equipamentos e sistemas do órgão.

É claro e evidente a essencialidade da continuidade da aquisição deste Antivírus para este Regional, com as características abaixo:

1.7.1. Console de gerenciamento centralizado;

1.7.2. Gerenciamento por grupos (integração com o Microsoft Active Directory);

1.7.3. Anti-malware/anti-vírus;

1.7.4. Anti-Ransomware;

1.7.5. IPS host;

1.7.6. IDS host;

1.7.7. Firewall host;

1.7.8. Filtro de conteúdo Web (classificação de site);

1.7.9. Suporte a Windows, iOS e Linux;

1.7.10. Proteção para solução de e-mail (Microsoft Exchange);

1.7.11. Gerenciamento de vulnerabilidades e correções;

1.7.12. Integração com soluções de SIEM;

1.7.13. Controle de dispositivos removíveis (USB);

1.7.14. Proteção proativa e instantânea contra ameaças desconhecidas;

1.7.15. Implementar técnicas de EDR (Endpoint Detection and Response).

1.7.16. As versões das licenças deverão ser as mais recentes disponibilizadas no mercado pelo fabricante.

1.7.17. As atualizações ou correções das versões das licenças serão realizadas durante todo o período de vigência contratual.

1.7.18. As soluções devem estar aderentes à infraestrutura tecnológica do CRCPA e serem compatíveis com os sistemas operacionais Microsoft Windows (64 bits), Linux e MacOS.

1.7.19. O detalhamento das especificações técnicas, encontra-se no **Anexo I**.

Demais requisitos necessários e suficientes à escolha da solução de TI

1.8. Portanto, a contratação deste serviço é fundamental para atender o público interno e externo, sendo assim, atendendo as atividades finalística institucionais e melhorando ainda mais a segurança dos dados deste regional, que visa atender a legislações da LGPD.

2 – ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

2.1. O registro do quantitativo de bens e serviços necessários para a composição do objeto a ser contratado está descrita no quadro abaixo item 2.1.2, de forma detalhada, motivada e justificada.

A contratação deverá ser realizada em conformidade com as legislações e normas pertinentes em vigor, em consonância com as justificativas formuladas no Documento de Oficialização de Demanda (DFD), nas quantidades e demais condições de execução a serem estabelecidas neste estudo e no PB/TR.

2.1.1. O quantitativo na tabela abaixo demonstra a necessidade do CRCPA, considerando o número de estações de trabalho, notebooks, servidores físicos e virtuais existentes no Regional, conforme demonstrado na tabela a seguir:

2.1.1 Descrições do Objeto.

Descrição	Qtidade.
Estações de Trabalho	35
Notebooks	23
Servidores físicos e Virtuais	03
Total	61

2.1.2 Descrições do Objeto.

ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	IDENTIFICAÇÃO CATSERV	UNIDADE DE MEDIDA	QUANTIDADE	VALOR MÁXIMO ACEITÁVEL
1	Kaspersky Next EDR Foundations	26077	-	70	R\$ 20.149,50

2.1.3 A modalidade dos itens acima consiste na aquisição de licenças de softwares, ou seja, as licenças não são de posse do comprador. A organização faz uso dos softwares como um aluguel e, portanto, é classificada como despesas de custeio.

Ao realizar a pesquisa de mercado, identifica-se uma latência nos valores contados em virtude da oscilação do mercado e principalmente na variação cambial do dólar.

2.2 Requisitos da Contratação

2.2.1. Requisitos necessários ao atendimento da necessidade:

2.2.1.1. A Renovação da licença Kaspersky EDR Foundations, que agora tem como acordo de forma a obter novas atualizações e suporte técnico especializado, conforme especificações contidas no Termo de Referência

2.2.1.2. A empresa contratada deverá realizar a implantação, customização, transição e adequação de base de dados (se houver), capacitação, alterações, manutenção e constante atualização do software às normas legais que disciplinam a matéria;

2.2.1.3. A CONTRATADA deverá executar todas as atividades, objeto deste Estudo, com base nas boas práticas de segurança da informação.

2.2.1.4. São requisitos exigidos com relação à Política de Segurança da Informação, devendo a CONTRATADA:

2.2.1.4.1. Obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pelo CRCPA e da LGPD;

2.2.1.4.2. Não veicular publicidade acerca dos serviços contratados, sem prévia autorização, por escrito, do CRCPA;

2.2.1.4.3. O serviço contratado deverá estar habilitado para funcionamento em rede com os sistemas operacionais especificados no ANEXO I.

2.2.1.5. Maiores detalhes das especificações técnicas encontram-se no Anexo I.

2.3 Requisitos de capacitação e treinamento dos usuários da solução

2.3.1. Considerando que se trata de uma solução para a qual a equipe de TI do CRCPA pode não ter conhecimentos técnicos suficientes para a operação, faz parte da solução a realização de treinamentos específicos.

2.3.2. Deve ser fornecido treinamento técnico-operacional tipo hands on e presencial, para 2 (dois) empregados do CRCPA, que cubram, preferencialmente em português e, alternativamente, em inglês:

a) a configuração e gerenciamento da solução;

b) técnicas de análise de erros e detecção de falhas de configuração, *debug* e *troubleshooting*;

2.3.3. Deve ser fornecido treinamento para 2 (dois) empregados do CRCPA, de no mínimo, 08 (oito) horas de duração.

2.4. Requisitos da Capacitação

2.4.2. Os treinamentos deverão ser presenciais tipo hands on e conduzidos por profissional qualificado pela fabricante, com a certificação (Certified Professional: Kaspersky EDR Foundations) da solução ofertada na proposta ou similar ao produto, com apresentação do correspondente documento de certificação, em versão original ou cópia autenticada 3, e que seja efetivo no quadro de funcionários de empresa pertencente ao programa de parceiros oficial da fabricante, com mais de 03 (três) anos de registro em CTPS e realizados nas dependências do Conselho Regional de Contabilidade do Pará.

2.4.2.1. A exigência da certificação do profissional é necessária para garantir a qualidade do treinamento e expertise para que, o profissional possua conhecimento da ferramenta do objeto do treinamento.

2.4.2.2. O treinamento deverá ser com a mesma base da versão dos softwares e hardwares da fabricante que serão instalados no CRCPA.

2.4.2.3. O material didático a ser utilizado no treinamento deverá ser disponibilizada pela empresa do fabricante e da mesma versão dos softwares e hardwares que serão instalados no CRCPA.

2.4.2.4. Todos os recursos necessários à efetiva prestação do treinamento, como: servidores, banco de dados, infraestrutura de rede de dados, entre outros, deverão ser disponibilizados pelo Cliente, uma vez que o treinamento será na sede do Conselho Regional de Contabilidade do Pará.

2.4.2.5. Todas as despesas com transporte, hospedagem, alimentação, locação de sala de aula (se necessário) e qualquer outra que seja necessária à efetiva realização do treinamento, são de responsabilidade da Contratada.

2.4.2.6. Os treinamentos deverão ser realizados de segunda à sexta-feira, em horário comercial.

3 – ANÁLISE DE SOLUÇÕES

Foi realizada pesquisas das soluções disponíveis no mercado de TI, chegando-se à conclusão que existem ferramentas em outras modalidades, sendo oferecida em vários tipos de aplicações, e que atendem às necessidades do objeto deste Estudo Técnico Preliminar, porém como a licença do antivírus que está em funcionamento em todos os computadores, servidores e notebooks deste Regional, é conveniente a renovação da licença, pois solução atende as necessidades deste Regional no quesito segurança dos dados e da rede e suas funcionalidades.

Por este motivo, não está sendo considerado neste ETP as demais soluções existentes no mercado.

Nesta situação, como é uma renovação de licença não cabe uma análise de outras soluções.

Para contratação em tela foram analisados processos similares aos dos Conselhos Federal de Contabilidade (CFC) e Conselho Regional de Engenharia e Agronomia De Mato Grosso (CREAMT), com objetivo de identificar a existência de novas metodologias, tecnologias ou inovações que melhor atendam às necessidades da Administração.

Por se tratar de objeto serviço comum, onde às especificações e padrões de desempenho e qualidade possam ser objetivamente definidos, conforme inciso XIII do art. 6º da Lei nº14.133/2021, com base em levantamento de mercado, o tipo de solução escolhida é a que mais se aproxima dos requisitos definidos e que mais promove a competição, levando em conta economicidade, eficácia, eficiência, padronização e práticas do mercado.

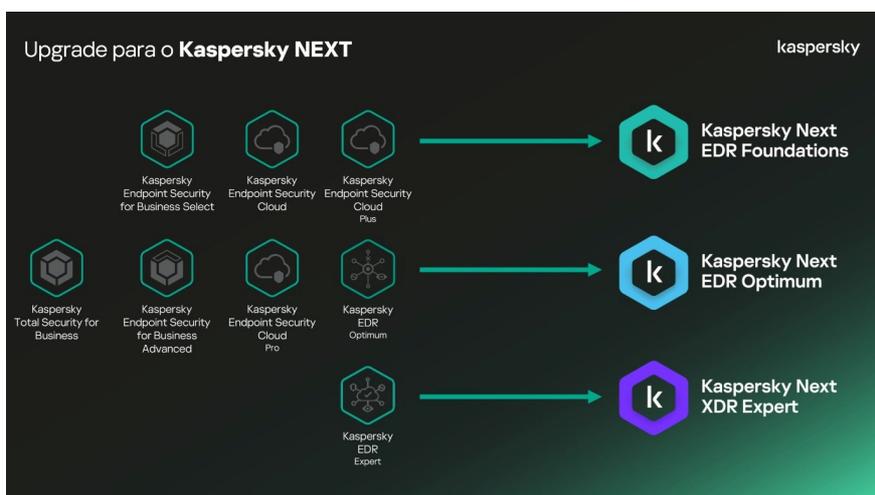
Convém ressaltar que o CRCPA tem acompanhado com atenção a jurisprudência emanada do Controle Externo, de modo a incorporar em seus processos de contratação os avanços e melhorias proporcionados pelo exame de casos concretos das aquisições de outros órgãos federais e em decorrência, obter contratações mais seguras e eficientes para esta Entidade. De forma que se entende caracterizada, no âmbito do Ministério da Justiça, a natureza de objeto comum da aquisição pretendida.

Diante do exposto, a dispensa de licitação se apresenta como melhor alternativa e vantajosidade de solução a ser contratada, proporcionando efetivos ganhos de eficiência ao Conselho, uma vez que será drasticamente reduzido o custo temporal e financeiro com o trâmite por dispensa de licitação, em consonância a Lei n.º 14.133/2021.

3.1 – IDENTIFICAÇÃO DAS SOLUÇÕES

Id	Descrição da solução (ou cenário)	Identificação Catser	Unid de Medida	Quantidade
1	Licença Kaspersky Next EDR Foundations	26077	Un	70

3.1.1 É importante registrar, que houve uma mudança na nomenclatura da Licença de uso, antes era chamado Kaspersky Endpoint Security for Business – Select e agora passou a se chamar com a nova linha Kaspersky Next EDR Foundations, conforme imagem abaixo.



<https://scansource.com.br/kaspersky/>

Foram avaliados duas alternativas para a contratação deste processo, tais como:

- **Cenário 01:** Aquisição da licença com direito de uso por 36 meses, com instalação/implantação, treinamento hands-on, suporte da fabricante no valor total R\$ 16.669,62;

- **Cenário 02:** Aquisição da licença com direito de uso por 36 meses, com instalação/implantação, treinamento hands-on, suporte da fabricante no valor total R\$ 21.474,40 e a prestação do serviço todos por 36 meses no valor R\$ 16.200,00 somados todo o cenário 02 o valor total seria de R\$ 37.674,40.

Abaixo temos um quadro demonstrativos com situações citadas a cima, sendo que, os valores apresentados no cenário 02 é superior ao cenário 01, avaliando que o custo benefício é mais vantajoso a contratação da licença por três anos sem a contratação da prestação do serviço. Enquanto que o valor da contratação da empresa com o serviço prestado é mais de 43% superior, tendo em vista a mão-de-obra agregada. Somando os valores pelo período de 36 meses o CRCPA estará economizando **R\$ 16.200,00**, tornando-se mais viável o **CENÁRIO 01**.

CENÁRIO 01

Serviço de Licença, treinamento e suporte fabricante

Id	Descrição da solução (ou cenário)	Identificação Catser	QTD de licenças	Valor Unitário	Valor Médio Total
1	Licença Kaspersky Next EDR Foundations	26077	70	R\$ 238,14	R\$ 16.669,62
				TOTAL	R\$ 16.669,62

CENÁRIO 02

Serviço de Licença, treinamento e suporte fabricante + Prestação de Serviço

Id	Descrição da solução (ou cenário)	Identificação Catser	QTD de licenças	Valor Unitário	Valor Total
1	Licença Kaspersky Next EDR Foundations	26077	70	538,21	R\$ 37.674,40
				TOTAL	R\$ 37.674,40

4- ANÁLISE DE SOLUÇÕES

4.1. Soluções Disponíveis no Mercado de TIC

4.1.1. Foi realizada uma pesquisa das soluções disponíveis no mercado de TI, chegando-se à conclusão que há mais de uma forma de contratação do serviço e aquisição, que atendem às necessidades do objeto deste Estudo Técnico Preliminar.

4.2. ANÁLISE DAS CONTRATAÇÕES ANTERIORES

4.2.1. O processo de contratação do referido antivírus, foi realizado em agosto de 2022, sendo contratada em setembro de 2022, devido à necessidade de renovação da licença. Sendo assim, é necessário a realização de um novo processo para aquisição do fornecimento de novas licenças, atualizadas de acordo com a versão mais nova para a segurança deste órgão.

4.3. Soluções de Mercado

Existem várias empresas no mercado que fornecem esse objeto, conforme demonstrado na tabela abaixo:

Empresa	CNPJ	Site/E-mail	Telefone
Techlead	11.887.021/0001-97	https://www.techlead.com.br/	(91)3222-9589.
Virtual Link	26.967.780/0001-37	https://www.virtuallink.com.br/	(91)98814-5238
Maw Solucoes Integradas	46.166.296/0001-16	marcos.vendas@outlook.com	(51)98576-3763
Solo Network	00.258.246/0001-68	https://www.danresa.com.br/	(41) 4062-6971

4.4. Contratações Públicas Similares

4.4.1. A fim de demonstrar que a presente contratação comum, foi efetuada pesquisa na internet com o objetivo de identificar contratações similares por órgãos públicos federais, estaduais ou instituições públicas.

4.4.2. Foram encontrados os seguintes editais/contratos:

Órgão	Objeto da Compra	Dados da Compra
CONSELHO FEDERAL DE CONTABILIDADE - UASG: 383500	Pregão Eletrônico - Aquisição de licenças de uso da solução de segurança antivírus Kaspersky Endpoint Security para estações de trabalho (endpoints). servidores e dispositivos móveis, gerenciados por solução centralizada no modelo onpremise. contemplando o serviço de implantação, o repasse de conhecimento hands-on, a manutenção preventiva/corretiva periódica, além da garantia, suporte técnico e atualizações por 36 (trinta e seis) meses.	Pregão Eletrônico Identificação da Compra: 90003/2024 Resultado: 10/05/2024
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DE MATO GROSSO CREA-MT- UASG: 389425	Renovação de Solução Corporativa de Antivírus, Kaspersky Next EDR Foundations Brazilian Edition com gerenciamento centralizado, e atualização contínua para execução em ambiente computacional, para atender as necessidade do CREA-MT.	Pregão Eletrônico Identificação da Compra: 90018/2024 Resultado: 05/06/2024

4.5. Outras Soluções Disponíveis

4.5.1. Esse item é aplicável especialmente para o caso de Solução de TIC que envolva desenvolvimento de software em que é necessário verificar se existe alternativa de solução nos órgãos da Administração, portanto, não se aplica a esta contratação.

4.6. A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública: O CRCPA teve como parâmetro contratos de serviços de Conselhos Federal de Contabilidade - CFC e Conselho Regionais de Engenharia e agronomia do Estado de Mato Grosso - CREAMT, tendo a constatação que é uma contratação vantajosa pela garantia da segurança que já é familiar o sistema de segurança, além de ser líder no mercado de segurança e contar com um laboratório de pesquisa no Brasil, que foi criado para detectar e analisar vírus e malwares locais conforme esta [fonte](#).

4.7. Portal do Software Público Brasileiro

Este item não é aplicável para a contratação objeto deste Estudo Técnico Preliminar.

4.8. Alternativa no Mercado de TIC

Há alternativa no mercado de TI. Vide subitem 3.1.

4.9. Modelo Nacional de Interoperabilidade (MNI)

Não se aplica ao contexto destes Estudos Preliminares.

4.10. Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)

Não se aplica ao contexto deste Estudo Preliminar.

4.11. Os diferentes modelos de prestação do serviço: existe a opção de contratação de prestação de serviço no aparelho e do serviço, porém o valor como apresentado no item 3.1, constata-se que o custo muito elevado, sendo assim, mais viável a aquisição da Cessão temporária de direitos sobre a licença;

4.12. Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes: haverá apenas uma solução conforme descrito no item 3.1;

4.13. A possibilidade de aquisição na forma de bens ou contratação como serviço: será na forma de contratação de serviço pelo período de 36 meses e tratado como serviço continuado, conforme Inciso 15 do art. VI combinado com o art. 106 da Lei nº14.133/2021.

4.14. A ampliação ou substituição da solução implantada: poderá ser feita, a depender da necessidade definida na gestão.

4.15. Portanto, é necessário frisar que, tão importante quanto efetuar a presente contratação, é garantir que as mesmas atendam aos melhores critérios técnicos sinalizados pelo mercado de Tecnologia da Informação, respeitando os princípios da economicidade, eficiência e eficácia de grande relevância para as ações governamentais, ao mesmo tempo em que subsidia a disponibilidade dos serviços de TI.

5 – REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Como já mencionado no texto item 3, outros regionais contratam este serviço, mas a depender do tamanho do número de funcionários e profissionais registrados no Conselho, existem contrato com valores mais elevados em decorrência de especificidades como sistemas e equipamentos com mais recursos e tipos diferentes de contratação.

6 – ANÁLISE COMPARATIVA DE CUSTOS (TCO)

6.1. Definição do método para a estimativa da configuração

6.1.1. O Serviço de Licença, treinamento e suporte fabricante do equipamento foi estimada com base no quadro abaixo, conforme quadro abaixo e item 2.1.1 do Cenário 01 e Cenário 02:

CENÁRIO 01

Serviço de Licença, treinamento e suporte fabricante

Id	Descrição da solução (ou cenário)	Identificação Catser	QTD
1	Kaspersky Next EDR Foundations Brazilian Edition 36 Meses - instalação/implantação - Suporte do fabricante	26077	70

6.2. Memória de Cálculo

6.2.1 Foi realizada pesquisa no mercado, com empresas que realizam o serviço objeto da contratação destes estudos preliminares e pesquisa em contratos na administração pública, conforme demonstrado na tabela a seguir:

		FORNECEDORES				ENTES PÚBLICOS				PNCP				
EMPRESAS		VIRTUAL LINK		SOLO NETWORK		TECHLEAD		CFC		CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DE MATO GROSSO				
		CNPJ:26.967.780/0001-37		CNPJ:00.258.246/0001-68		CNPJ:07.166.562/0001-59		CNPJ: 15126437000143		CNPJ: 46.166.296/0001-16				
		CONTATO : https://www.virtuallink.com.br/		CONTATO : (48) 3224-0416		CONTATO : (48) 3224-0416		CONTATO: (61) 2022-8002		CONTATO: (51) 98576-3763				
		EMAIL: comercial@virtuallink.com.br		EMAIL: rafael.lehmkuhl@solonetwork.com.		EMAIL: rafael.lehmkuhl@solonetwork.com.		EMAIL: contabilidade.sede@ebsrh.gov.br		EMAIL: marcos.vendas@outlook.com				
ITEM	Treinamento	Qtde	Preço Unitário		Preço Total		Preço Unitário		Preço Total		Preço Unitário		Preço Total	
			VALOR	VALOR	VALOR	VALOR	VALOR	VALOR	VALOR	VALOR	VALOR	VALOR	VALOR	VALOR
1	Kaspersky Next EDR Foundations Brazilian Edition 36 Meses - instalação/implantação - Suporte do fabricante	70	R\$ 306,78	R\$ 21.474,40	R\$ 225,65	R\$ 15.795,50	R\$ 287,85	R\$ 20.149,50	R\$ 215,41	R\$ 15.078,70	R\$ 155,00	R\$		
			R\$ 21.474,40		R\$ 15.795,50		R\$ 20.149,50		R\$ 15.078,70		R\$		#REF!	

6.2.2. A pesquisa de preço para fins de determinação do preço estimado para o objeto deste estudo técnico preliminar, foi realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada: Pannel de preço/ PNCP do Conselho Regional de Engenharia e Agronomia do Mato Grosso – CREA/MT, propostas apresentadas pelas empresas Virtual Link, Techlead e Solo Network, nos e Entes Públicos Conselho Federal de Contabilidade - CFC, com base no inciso I, II e IV, do artigo 5º da Instrução Normativa nº 65, de 07/07/2021, da Secretaria Especial de Desburocratização, Gestão e Governo Digital, do Ministério da Economia.

I - Pannel de Preços e PNCP, disponível no endereço eletrônico gov.br/pannel de preços, desde que as cotações se refiram a aquisições ou contratações firmadas no período de até 1 (um) ano anterior à data de divulgação do instrumento convocatório;

II - Aquisições e contratações similares de outros entes públicos, firmadas no período de até 1 (um) ano anterior à data de divulgação do instrumento convocatório.

IV - Pesquisa direta com fornecedores, mediante solicitação formal de cotação, desde que os orçamentos considerados estejam compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do instrumento convocatório.

6.2.3. Foram verificados contratos no portal da transparência entes Públicos, com o mesmo objeto. Foram solicitadas propostas de 3 (três) empresas, todas enviaram e estavam de acordo com as especificações técnicas.

6.2.4. A pesquisa no Portal Nacional de Contratações Públicas (https://pncp.gov.br/app/editais?q=&status=recebendo_proposta&pagina=1) apresentou resultado próximos para a contratação do serviço em tela. Portanto, foi considerado, a pesquisa realizada com PNCP de entes públicos.

6.3 – IDENTIFICAÇÃO DAS SOLUÇÕES

ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	IDENTIFICAÇÃO CATSERV	QTIDADE
1	Kaspersky Next EDR Foundations Brazilian Edition 36 Meses - instalação/implantação - Suporte do fabricante	26077	70

6.2.1. A solução consiste na contratação de Aquisição de licença de uso do Kaspersky Next EDR Foundations Brazilian Edition 36 Meses - instalação/implantação - Suporte do fabricante, configuração e treinamento presencial tipo hands on da solução, com suas políticas de segurança e com as características discriminadas, conforme exposto no ITEM 2.2 à 3.1 do Cenário 01 e termo de referência.

7. ESTIMATIVA DO CUSTO TOTAL DA CONTRATAÇÃO

7.1. O custo total da demanda é de **médio R\$ 16.669,62** (dezesesseis mil e seiscentos e sessenta e nove e seis reais e sessenta e dois centavos).

7.2. Para Estimativa do custo total da demanda, realizou-se pesquisa conforme informado no item 6.2.

7.3. Para a contratação objeto deste estudo preliminar, a efetuada pesquisa realizada resultou em formação de planilha média para a contratação do serviço.

7.4. O Pagamento é mensal pelo período de 12 meses.

7.5. O reajuste do contrato poderá ser efetuado por meio de reajuste de preços, conforme previsto no Item I do Art.136 da lei 14.133/21, considerando-se a aplicação do índice de reajustamento IPCA (Índice de Preços ao Consumidor Amplo), mediante a aplicação da seguinte fórmula (art. 5º do Decreto n.º 1.054, de 1994):

$R = V (I - I^0) / I^0$, onde:

R = Valor do reajuste procurado;

V = Valor contratual do serviço a ser reajustado;

Iº = índice inicial - refere-se ao índice de custos ou de preços correspondente à data fixada para entrega da proposta da licitação;

I = Índice relativo ao mês do reajustamento;

8 – DECLARAÇÃO DA VIABILIDADE DA CONTRATAÇÃO

8.1. Foram analisadas contratações análogas na Administração Pública Federal contemplando as mesmas subscrições objeto da contratação pretendida pelo CRCPA, porém em quantidades menores ou maiores.

8.2. Assim, considerando as contratações analisadas, verificamos que a aquisição objeto deste estudo técnico preliminar é viável.

9 – DEMONSTRATIVOS DOS RESULTADOS PRETENDIDOS

9.1. Dentre os resultados, espera-se:

9.1.1. manter a qualidade da prestação dos serviços de TI, proporcionando um ambiente adequado do CRCPA;

9.1.2. dotar o CRCPA com uma base tecnológica atual e eficiente, capaz de atender às exigências de qualidade, alta disponibilidade e alto desempenho operacional;

9.1.3. prover uma melhor configuração na redundância do acesso aos sistemas informatizados e à rede mundial de computadores, diminuindo o risco de falta de conectividade e de segurança, ao mesmo tempo que aumenta a resiliência do acesso à rede corporativa;

9.1.4. que a contratação decorrente deste estudo acarrete para o CRCPA os menores custos possíveis na obtenção da proposta mais vantajosa a ser cobrada pela contratação do serviço objeto deste Estudo Técnico Preliminar.

9.2. A motivação da contratação da solução de proteção de rede, é assegurar o provimento de Infraestrutura de TI segura e adequada para que as áreas finalísticas do negócio do CRCPA continuem operacionais; aumentando a eficiência da infraestrutura de TI do CRCPA, reduzindo os custos e simplificando o gerenciamento;

9.3. Contribuir para garantia de um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;

9.4. Oferecer maior agilidade e eficácia no tratamento de incidentes envolvendo endpoints (estações de trabalho e notebooks) comprometidos;

9.5. Evitar, mitigar e conter a propagação de pragas digitais facilitando o tratamento destes incidentes (vírus /malwares/spywares, spam, dentre outros) com a administração centralizada da solução de proteção;

9.6. Permitir o controle de acesso à rede por dispositivos computacionais, permitindo gerenciamento destes dispositivos;

9.7. Gerar economicidade e melhoria de qualidade do serviço de proteção de endpoints;

9.8. Mitigar riscos de infecção na transição entre soluções de antivírus;

9.9. É importante frisar que, tão importante quanto efetuar a presente contratação, é garantir que a mesma atenda aos melhores critérios técnicos e de segurança sinalizados pelo mercado de Tecnologia da Informação, respeitando os princípios da economicidade, eficiência e eficácia de grande relevância para as ações governamentais, ao mesmo tempo que subsidia a disponibilidade dos serviços de TI;

9.10. Espera-se, também, que os serviços a serem suportados pelos serviços de gerenciamento de ambiente de TI permitam proporcionar a capacidade do CRCPA em disponibilizar serviços com segurança e qualidade, segundo os objetivos estratégicos listados no Planejamento Estratégico do Sistema CFC/CRCs (2018-2027) e na versão 1.1 do Plano Diretor de Tecnologia da Informação (PDTI) do CRCPA, biênio 2024-2025.

9.2. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO, QUANDO NECESSÁRIA PARA A INDIVIDUALIZAÇÃO DO OBJETO

9.2.1. O parcelamento da solução não é viável, tendo em vista que, o contrato dispõe de apenas um item não é viável o parcelamento deste para a execução do contrato, nesse sentido, a padronização do serviço contratados é imprescindível, pois assim se evita possíveis ocorrências de incompatibilidades de suprimentos.

10 – FISCALIZAÇÃO DO CONTRATO

10.1. A fiscalização do contrato será realizada por fiscal efetivo ou fiscal substituto designado pela Administração, dentre os empregados do Conselho Regional de Contabilidade do Pará.

10.2. Não há a necessidade de capacitação específica para os funcionários que irão atuar como fiscais do contrato.

11 – LEVANTAMENTO DOS ELEMENTOS ESSENCIAIS DO TERMO DE REFERÊNCIA

11.1. O Termo de Referência para Aquisição de licença de uso do Kaspersky Next EDR Foundations Brazilian Edition 36 Meses - instalação/implantação - Suporte do fabricante, configuração e treinamento presencial tipo hands on da solução, com suas políticas de segurança e com as características discriminadas, conforme exposto no ITEM 2.2 á 3.1 do Cenário 01 e termo de referência. A solução deve integrar instalação e configuração e prover, pelo período de 36 (trinta e seis) meses, suporte técnico do fabricante 24X7 (vinte e quatro horas por dia, sete dias por semana), incluindo a substituição de peças e equipamentos defeituosos (se houver necessidade), manutenção evolutiva, preventiva e corretiva, licenças e assinaturas pertinentes, deverá seguir a seguinte estrutura e contará com, no mínimo, com os itens discriminados no art. 12, da Instrução Normativa n.º 1, da Secretaria de Governo Digital/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Ministério da Economia, de 4 de abril de 2019, a saber::

a) definição do objeto da contratação;

b) código(s) do Catálogo de Materiais (Catmat) ou do Catálogo de Serviços (Catsr) relacionado(s) a cada item da contratação, disponíveis no Portal de Compras do Governo Federal;

c) descrição da solução de TIC;

d) justificativa para contratação da solução;

e) especificação dos requisitos da contratação;

f) definição das responsabilidades da contratante, da contratada e do órgão gerenciador da Ata de Registro de Preços, quando aplicável;

g) modelo de execução e gestão do Contrato;

h) estimativas de preços da contratação;

i) adequação orçamentária e cronograma físico-financeiro, caso necessário;

j) regime de execução do contrato;

k) critérios técnicos para seleção do fornecedor;

l) índice de correção monetária, quando for o caso.

9 – ASSINATURAS

A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 121, de 03 de junho de 2024.

Conforme o § 2º do Art. 10 da IN SGD/ME nº 94, de 2022, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TI:

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
--------------------	-------------------------

_____ Newton da Silva Junior Matrícula: 0029	_____ Luciano Coutinho Almeida Matrícula: 0019
--	--

10 – APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

AUTORIDADE MÁXIMA DA ÁREA DE TIC
_____ Ewerton Ribeiro Jorge Vice-Presidente de Administração



Documento assinado eletronicamente por **Luciano Coutinho Almeida, Analista - Sistemas / Desenvolvimento**, em 16/08/2024, às 15:23, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Newton da Silva Junior, Analista - Sistemas / Desenvolvimento**, em 16/08/2024, às 15:24, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Ewerton Ribeiro Jorge, Vice-Presidente**, em 23/08/2024, às 10:35, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0462548** e o código CRC **9131E514**.



CONSELHO REGIONAL DE CONTABILIDADE DO PARÁ

Rua Avertano Rocha, 392, - Bairro Comércio, Belém/PA, CEP 66023-120 Telefone: (91) 3202-4150 - www.crcpa.org.br

E-mail: crcpa@crcpa.org.br

Processo n.º : 9079612110000416.000012/2024-81

ANEXO A MODELO DE ORDEM DE SERVIÇO

ORDEM DE SERVIÇO						
1 – IDENTIFICAÇÃO						
Ordem de Serviço						
Contrato Nº:						
Contratada:						
Data da Emissão:		Área Requisitante do Serviço:				
Usuário Solicitante:						
E-mail:		Telefone:				
Solução de TI:						
2 – ESPECIFICAÇÃO DOS PRODUTOS/SERVIÇOS E VOLUMES ESTIMADOS						
Item	Descrição do Produto ou Serviço	Métrica	Valor Unit. (R\$)	Quantidade/ Volume	Valor Total (R\$)	
TOTAL						
3 - INSTRUÇÕES COMPLEMENTARES						
4 - CRONOGRAMA						
Item referente ao Produto/Serviço				Início Previsto	Fim Previsto	Prazo Máximo
5 - ARTEFATOS / PRODUTOS						
Fornecidos			A serem gerados e/ou atualizados			

(*) Modelo meramente exemplificativo



CONSELHO REGIONAL DE CONTABILIDADE DO PARÁ

Rua Avertano Rocha, 392, - Bairro Comércio, Belém/PA, CEP 66023-120 Telefone: (91) 3202-4150 - www.crcpa.org.br
E-mail: crcpa@crcpa.org.br

Processo n.º : 9079612110000416.000012/2024-81

1. INFORMAÇÕES SIGILOSAS 1.1. Para os propósitos deste Instrumento são "Informações Sigilosas" todos e quaisquer dados e informações verbais, digitais ou na forma escrita em meio físico referentes à estratégia, administração, processos e suas representações gráficas, ou atividades-fim do CONSELHO REGIONAL DE CONTABILIDADE DO PARÁ, doravante denominado CRCPA, incluindo dados e informações oriundos do relacionamento do CRCPA com seus empregados e colaboradores, com sua base de profissionais da contabilidade, atuais e em prospecção, que possam envolver suas estratégias, informações financeiras, pessoais, operacionais, econômicas, técnicas, jurídicas, planos comerciais, de marketing, de programação, bem como demais informações institucionais ou "know-how", que não são de conhecimento público, e que tenham sido, ou seja, direta ou indiretamente fornecidos, disponibilizados ou divulgados pelo CRCPA, seus empregados, fornecedores ou seus representantes legais em decorrência do Contrato n.º _____.

1.2. O compromisso assumido neste Termo de Confidencialidade abrange todas as obrigações referentes a sigilo previstas no EDITAL

2. UTILIZAÇÃO DA INFORMAÇÃO SIGILOSA

2.1. O signatário reconhece que as informações a serem acessadas são vitais para o sucesso dos serviços e serão revestidas de sigilo e confidencialidade e sua divulgação ou uso indevido poderá acarretar em perdas e danos, de acordo com os preceitos legais aplicáveis à matéria. 2.2. Sem o consentimento prévio por escrito do CRCPA, o signatário não poderá reproduzir ou copiar, no todo ou em parte, em qualquer meio - físico ou digital - quaisquer Informações Sigilosas que direta ou indiretamente tenha tido acesso.

2.3. Sem o consentimento prévio por escrito do CRCPA, o signatário não revelará ou divulgará a terceiros, no todo ou em parte, quaisquer Informações Sigilosas que direta ou indiretamente tenha tido acesso.

2.4. A qualquer tempo, poderá ocorrer a suspensão do fornecimento das Informações Sigilosas, bem como o acesso às mesmas, por iniciativa do CRCPA, sendo certo que tal suspensão não afetará as obrigações aqui previstas.

3. DIVULGAÇÃO DE INFORMAÇÃO SIGILOSA EM VIRTUDE DE IMPOSIÇÃO LEGAL

3.1. Se o signatário for legalmente obrigado a revelar, no todo ou em parte, as Informações Sigilosa por qualquer juízo ou autoridade governamental competente, deverá enviar prontamente ao CRCPA aviso por escrito com prazo suficiente para permitir que esta adote as medidas legais cabíveis para resguardo de seus direitos.

4. PRAZO DE VALIDADE

4.1. Este compromisso tem natureza irretratável e irrevogável e vigorará por prazo indeterminado.

5. RELACIONAMENTO ENTRE AS PARTES

5.1 Este instrumento não cria vínculo de relação trabalhista com o CRCPA nem outro relacionamento de qualquer espécie.

6. FORO

6.1. Este documento será regido e interpretado pelas Leis da República Federativa do Brasil, sendo eleito o foro da Justiça Federal do Distrito Federal, para dirimir os litígios, controvérsias e disputas relacionadas ou decorrentes do presente Termo, com exclusão de qualquer outro, por mais privilegiado que seja.

[Local] ____ de _____ de ____

Assinatura: _____

Nome:

RG:

CPF:

Observação: Emitir em papel que identifique a licitante

1. INFORMAÇÕES SIGILOSAS 1.1. Para os propósitos deste Instrumento são "Informações Sigilosas" todos e quaisquer dados e informações verbais, digitais ou na forma escrita em meio físico referentes à estratégia, administração, processos e suas representações gráficas, ou atividades-fim do CONSELHO REGIONAL DE CONTABILIDADE DO PARÁ, doravante denominado CRCPA, incluindo dados e informações oriundos do relacionamento do CRCPA com seus empregados e colaboradores, com sua base de profissionais da contabilidade, atuais e em prospecção, que possam envolver suas estratégias, informações financeiras, pessoais, operacionais, econômicas, técnicas, jurídicas, planos comerciais, de marketing, de programação, bem como demais informações institucionais ou "know-how", que não são de conhecimento público, e que tenham sido, ou seja, direta ou indiretamente fornecidos, disponibilizados ou divulgados pelo CRCPA, seus empregados, fornecedores ou seus representantes legais em decorrência do Contrato nº _____.

1.2. O compromisso assumido neste Termo de Confidencialidade abrange todas as obrigações referentes a sigilo previstas no EDITAL

2. UTILIZAÇÃO DA INFORMAÇÃO SIGILOSA

2.1. O signatário reconhece que as informações a serem acessadas são vitais para o sucesso dos serviços e serão revestidas de sigilo e confidencialidade e sua divulgação ou uso indevido poderá acarretar em perdas e danos, de acordo com os preceitos legais aplicáveis à matéria. 2.2. Sem o consentimento prévio por escrito do CRCPA, o signatário não poderá reproduzir ou copiar, no todo ou em parte, em qualquer meio - físico ou digital - quaisquer Informações Sigilosas que direta ou indiretamente tenha tido acesso.

2.3. Sem o consentimento prévio por escrito do CRCPA, o signatário não revelará ou divulgará a terceiros, no todo ou em parte, quaisquer Informações Sigilosas que direta ou indiretamente tenha tido acesso.

2.4. A qualquer tempo, poderá ocorrer a suspensão do fornecimento das Informações Sigilosas, bem como o acesso às mesmas, por iniciativa do CRCPA, sendo certo que tal suspensão não afetará as obrigações aqui previstas.

3. DIVULGAÇÃO DE INFORMAÇÃO SIGILOSA EM VIRTUDE DE IMPOSIÇÃO LEGAL

3.1. Se o signatário for legalmente obrigado a revelar, no todo ou em parte, as Informações Sigilosa por qualquer juízo ou autoridade governamental competente, deverá enviar prontamente ao CRCPA aviso por escrito com prazo suficiente para permitir que esta adote as medidas legais cabíveis para resguardo de seus direitos.

4. PRAZO DE VALIDADE

4.1. Este compromisso tem natureza irretratável e irrevogável e vigorará por prazo indeterminado.

5. RELACIONAMENTO ENTRE AS PARTES

5.1 Este instrumento não cria vínculo de relação trabalhista com o CRCPA nem outro relacionamento de qualquer espécie.

6. FORO

6.1. Este documento será regido e interpretado pelas Leis da República Federativa do Brasil, sendo eleito o foro da Justiça Federal do Distrito Federal, para dirimir os litígios, controvérsias e disputas relacionadas ou decorrentes do presente Termo, com exclusão de qualquer outro, por mais privilegiado que seja.

[Local] ____ de _____ de ____

Assinatura: _____

Nome:

RG:

CPF:

Observação: Emitir em papel que identifique a licitante



CONSELHO REGIONAL DE CONTABILIDADE DO PARÁ

Rua Avertano Rocha, 392, - Bairro Comércio, Belém/PA, CEP 66023-120 Telefone: (91) 3202-4150 - www.crcpa.org.br
E-mail: crcpa@crcpa.org.br

Processo n.º : 9079612110000416.000012/2024-81

1. O Instrumento de Medição de Resultado define os índices a serem atingidos para o cumprimento do conjunto de compromissos acordados entre Contratante e a Contratada.
2. Tais índices serão medidos e aplicados aos serviços contratados pelo Conselho Regional de Contabilidade do Pará e prestados pela Contratada.
3. Mensalmente/ ou quando necessário de acordo com o TR os dados do IMR deverão ser apresentados ao Conselho Regional de Contabilidade do Pará, incluindo informações sobre ações e necessidades para a correção de desvios, visando atingir, manter e melhorar os níveis desejados. A abrangência e o nível de detalhamento dos demonstrativos serão definidos conforme as necessidades identificadas pela CONTRATADA, podendo sofrer alterações ao longo do tempo, as quais serão encaminhadas ao Conselho Regional de Contabilidade do Pará via os processos de Gerenciamento do Instrumento de Medição de Resultado e de Mudanças do mesmo. Para a medição dos índices de nível de resultados, serão considerados os seguintes conceitos:
4. Atendimento local/remoto: atendimentos realizados nas dependências do Conselho Regional de Contabilidade do Pará pela equipe da CONTRATADA;
5. Horário padrão de atendimento: O atendimento padrão será realizado 05 (cinco) dias por semana, 8 (oito) horas por dia (horário de expediente do CRCPA), durante todo o ano.
6. Instrumento regulado pela Instrução Normativa SEGES-MP nº 05, de maio de 2017 e alterada pela IN nº 49/2022, que cria parâmetros para a efetivação de pagamento por resultados, possibilitando à Administração Pública remunerar o fornecedor na medida do cumprimento do nível de serviços pactuado no instrumento, visando, em última análise, à obtenção dos melhores resultados e da máxima qualidade e eficiência na prestação dos serviços, contribuindo para evitar contratações infrutíferas e o dispêndio irregular de recursos públicos. O IMR aplicado ao atual Termo de Referência se dá nos seguintes termos:

Os seguintes níveis de IMR devem ser atendidos:

INDICADOR 1	
Prazo para atendimento às solicitações demandadas à CONTRATADA	
Item	Descrição
Finalidade:	Garantir os padrões de atendimento às solicitações do Conselho Regional de Contabilidade do Pará
Meta a cumprir:	99% dos atendimentos solucionados no prazo previsto conforme nível de severidade

Instrumento de medição:	Abertura e fechamento de chamado.
Forma de acompanhamento:	Medição via ferramenta da CONTRATADA e relatórios mensais de acompanhamento. Os tempos serão registrados e apurados através do Sistema de Service Desk da CONTRATADA.
Periodicidade:	Mensal - 24 x 7
Mecanismo de Cálculo:	HP= Quantidade de horas de previstas de um serviço em um determinado período de tempo T. HE = Quantidade total de horas executadas de um determinado período de tempo T. R = HE-HP
Início de Vigência:	Data da assinatura do contrato.
Faixas de ajuste no pagamento:	Situação Readequação valor de Ordem de Serviço ou pendência; X <= 8 horas 100% do valor da OS X > 8 h e X <= 12 h 95% do valor da OS X > 12 h e X <= 16 h 90% do valor da OS X > 16 h e X <= 20 h 85% do valor da OS X > 20 h x <= 24h 80 % do valor da OS
Sanções	Se X > 24 e X <= 28h, multa de 1% sobre a fatura do período. Se X > 28h e X <= 32h, multa de 2% sobre a fatura do período. Se X > 32h, multa de 3% sobre a fatura do período + direito de rescisão contratual pela Contratante.
Observações	Não serão aplicadas glosas durante os primeiros 90 dias após a implantação do serviço, por se tratar de período de adaptação contratual. Nos três primeiros meses do contrato, as Glosas, caso existam, poderão ser convertidas em advertências, visando adaptação à sistemática

INDICADOR 2	
Prazo para atendimento às solicitações ERROS de Sistema	
Item	Descrição
Finalidade:	Garantir os padrões de qualidade dos sistemas utilizados pelo Conselho Regional de Contabilidade do Pará
Meta a cumprir:	99,4% dos atendimentos solucionados no prazo previsto conforme nível de severidade
Instrumento de medição:	Abertura e fechamento de chamado.
Forma de acompanhamento:	Medição via ferramenta da CONTRATADA e relatórios mensais de acompanhamento. Os tempos serão registrados e apurados através do Sistema de Service Desk da CONTRATADA.
Periodicidade:	Mensal - 24 x 7

Mecanismo de Cálculo:	HP= Quantidade de horas de previstas de um serviço em um determinado período de tempo T. HE = Quantidade total de horas executadas de um determinado período de tempo T. R = HE-HP
Início de Vigência:	Data da assinatura do contrato.
Faixas de ajuste no pagamento:	Situação Readequação de valor do licenciamento mensal; X <= 4 horas 100% do valor do licenciamento mensal; X > 4 h e X <= 12 h 95% do valor do licenciamento mensal; X > 12 h e X <= 16 h 90% valor do licenciamento mensal; X > 16 h e X <= 20 h 85% valor do licenciamento mensal; X > 20 h x <= 24h 80 % do valor do licenciamento mensal;
Sanções	Se X > 24 e X <= 28h, multa de 1% sobre a fatura do período. Se X > 28h e X <= 32h, multa de 2% sobre a fatura do período. Se X > 32h, multa de 3% sobre a fatura do período + direito de rescisão contratual pela Contratante.
Observações	Não serão aplicadas glosas durante os primeiros 90 dias após a implantação do serviço, por se tratar de período de adaptação contratual. Nos três primeiros meses do contrato, as Glosas, caso existam, poderão ser convertidas em advertências, visando adaptação à sistemática.

O Conselho Regional de Contabilidade do Pará entende que haverá uma fase inicial de transição e adequação dos processos de atendimento por parte da Contratada. Sendo assim, os níveis de serviço do (IMR) não serão exigidos contratualmente durante os primeiros 45 (quarenta e cinco) dias de duração do contrato. Os índices deverão ser apurados e apresentados ao Conselho Regional de Contabilidade do Pará no entanto a Contratada não estará sujeita a penalidades pelo seu descumprimento durante este período.

7. Ressalta-se ainda que a Contratada não poderá ser penalizada (multada) em mais de 30% (trinta por cento) do valor de sua fatura mensal em qualquer mês, por descumprimento dos níveis de serviço acordados. Todavia, o Conselho Federal de Contabilidade resguarda o direito de cancelar o contrato unilateralmente caso os índices não sejam atingidos por 03 (três) meses consecutivos.



CONSELHO REGIONAL DE CONTABILIDADE DO PARÁ

Rua Avertano Rocha, 392, - Bairro Comércio, Belém/PA, CEP 66023-120 Telefone: (91) 3202-4150 - www.crcpa.org.br E-mail: crcpa@crcpa.org.br
Processo n.º : 9079612110000416.000012/2024-81

IDENTIFICAÇÃO

PROCESSO	9079612110000416.000012/2024-81	Nº DA OS / CS:	
OBJETO:	Solução de Appliance Fortinet e licença de uso da solução de análise de fluxo de rede com recursos de segurança e conexão avançada, incluindo serviços de instalação, configuração, treinamento e suporte técnico e garantia por 36 meses		
CONTRATANTE:	CRCPA		
CONTRATADA			

Por este instrumento, atestamos, para fins de cumprimento do disposto no art. 19, inciso II, alínea "a" da Instrução Normativa nº 94, de 23 de dezembro de 2022, emitida pelo Ministério da Economia/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Secretaria de Governo Digital, que os serviços (ou bens), relacionados na O.S.(Ordem de Serviço) ou C.S. (Contrato Simplificado) acima identificada, foram recebidos nesta data e serão objetos de avaliação quanto à conformidade de qualidade, de acordo com os Critérios de Aceitação previamente definidos pela Contratante.

Ressaltamos que o recebimento definitivo destes serviços (ou bens) ocorrerá em até ___ dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Termo de Referência correspondente ao Contrato supracitado.

De Acordo

CONTRATANTE	CONTRATADA
Gestor do Contrato	Responsável pela Contratada
<hr/> <p>< Nome > Matrícula: < Matr.></p>	<hr/> <p>< Nome > < Qualificação.></p>

Belém (PA), _____, de _____ de 20__.



CONSELHO REGIONAL DE CONTABILIDADE DO PARÁ

Rua Avertano Rocha, 392, - Bairro Comércio, Belém/PA, CEP 66023-120 Telefone: (91) 3202-4150 - www.crcpa.org.br E-mail: crcpa@crcpa.org.br
Processo n.º : 9079612110000416.000012/2024-81

IDENTIFICAÇÃO

CONTRATO		Nº DA OS / CS:	
OBJETO:			
CONTRATANTE:			
CONTRATADA			

Por este instrumento, atestamos, para fins de cumprimento do disposto no art. 19, inciso II, alínea "a" da Instrução Normativa nº 94, de 23 de dezembro de 2024, emitida pelo Ministério da Economia/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Secretaria de Governo Digital, que os serviços (ou bens), relacionados na O.S.(Ordem de Serviço) ou C.S. (Contrato Simplificado) acima identificada foram formalmente devidamente avaliados e atendem aos requisitos estabelecidos no Termo de Referencia do Contrato acima referenciado.

De Acordo

CONTRATANTE	CONTRATADA
Gestor do Contrato	Responsável pela Contratada
<hr/> <p>< Nome> Matrícula: < Matr.></p>	<hr/> <p>< Nome> < Qualificação.></p>

Belém (PA), _____, de _____ de 20__.



CONSELHO REGIONAL DE CONTABILIDADE DO PARÁ
Rua Avertano Rocha, 392, - Bairro Comércio, Belém/PA, CEP 66023-120
Telefone: (91) 3202-4150 - www.crcpa.org.br E-mail: crcpa@crcpa.org.br

MINUTA DE CONTRATO

Processo nº 9079612110000416.000012/2024-81

TERMO DE CONTRATO Lei nº 14.133, de 1º de abril de 2021

CONSELHO REGIONAL DE CONTABILIDADE DO PARÁ

(Processo Administrativo nº 9079612110000416.000012/2024-81)

CONTRATO ADMINISTRATIVO
Nº/....., QUE FAZEM
ENTRE SI A UNIÃO, POR
INTERMÉDIO DO (A)

.....
E
.....

1. A Autarquia Especial, Conselho Regional de Contabilidade do Pará - CRCPA, com sede no(a) Rua Avertano Rocha, 392, na cidade de Belém /Estado do Pará, inscrito(a) no CNPJ sob o nº 04.977.518/0001-30, neste ato representado(a) pelo(a) Ailton Ramos Correa Junior (Presidente), nomeado(a) pela Ata Plenária Ordinária nº 809, de 03 de janeiro de 2024, doravante denominado **CONTRATANTE**, e o(a) inscrito(a) no CNPJ/MF sob o nº, sediado(a) na, doravante designado **CONTRATADO**, neste ato representado(a) por (nome e função no contratado), conforme atos constitutivos da empresa OU procuração apresentada nos autos, tendo em vista o que consta no Processo nº 9079612110000416.000003/2024-90 e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente da Dispensa Eletrônica n. XX/2024, mediante as cláusulas e condições a seguir enunciadas.

1.1. CLÁUSULA PRIMEIRA – OBJETO (art. 92, I e II)

1.2. O objeto do presente instrumento é a contratação de solução de tecnologia da informação e comunicação de Aquisição das licenças de uso da solução de segurança antivírus Kaspersky Endpoint Security for Business - Select, para estações de trabalho (endpoints), servidores e dispositivos móveis, gerenciados por solução centralizada no modelo on-premise, contemplando o serviço de implantação, treinamento hands-on (presencial), além da garantia, suporte técnico e atualizações por 36 (trinta e seis) meses do Fabricante, nas condições estabelecidas no Termo de Referência.

1.3. Objeto da contratação:

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Kaspersky Next EDR Foundations	26077	UND	70		

1.4. Vinculam esta contratação, independentemente de transcrição:

- 1.4.1. O Termo de Referência;
- 1.4.2. O Aviso da Dispensa Eletrônica;
- 1.4.3. A Proposta do contratado;
- 1.4.4. Eventuais anexos dos documentos supracitados.

CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 36 meses, contados da assinatura do contrato, na forma dos artigos 105 da Lei nº 14.133, de 2021.

2.1.1. O prazo de vigência será automaticamente prorrogado, independentemente de termo aditivo, quando o objeto não for concluído no período firmado acima, ressalvadas as providências cabíveis no caso de culpa do contratado, previstas neste instrumento.

3. CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS (art. 92, IV, VII e XVIII)

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

4. CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. Não será admitida a subcontratação do objeto contratual.

CLÁUSULA QUINTA - PREÇO

5.1. O valor mensal da contratação é de R\$ (.....), perfazendo o valor total de R\$ (.....).

OU

5.2. O valor total da contratação é de R\$..... (.....)

5.3. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

5.4. O valor acima é meramente estimativo, de forma que os pagamentos devidos ao contratado dependerão dos quantitativos efetivamente fornecidos.

6. CLÁUSULA SEXTA - PAGAMENTO (art. 92, V e VI)

6.1. O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

CLÁUSULA SÉTIMA - REAJUSTE (art. 92, V)

- 7.1. Os preços inicialmente contratados são fixos e irrevogáveis no prazo de um ano contado da data do orçamento estimado, em __/__/__ (DD/MM/AAAA).
- 7.2. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.
- 7.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.
- 7.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).
- 7.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).
- 7.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.
- 7.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.
- 7.8. O reajuste será realizado por apostilamento.

CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE (art. 92, X, XI e XIV)

- 8.1. São obrigações do Contratante, além das previstas no termo de referência:
- 8.2. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;
- 8.3. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;
- 8.4. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;
- 8.5. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;
- 8.6. Comunicar a empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;
- 8.7. Efetuar o pagamento ao Contratado do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;
- 8.8. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;
- 8.9. Identificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;
- 8.10. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.
- 8.11. A Administração terá o prazo de 30 dias, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.
- 8.12. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 dias.
- 8.13. Comunicar o Contratado na hipótese de posterior alteração do projeto pelo Contratante, no caso [do art. 93, §2º, da Lei nº 14.133, de 2021](#).
- 8.14. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO (art. 92, XIV, XVI e XVII)

- 9.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas, além das previstas no termo de referência:
- 9.2. Manter preposto aceito pela Administração no local ou do serviço para representá-lo na execução do contrato.
- 9.3. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.
- 9.4. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior ([art. 137, II](#)) e prestar todo esclarecimento ou informação por eles solicitados;
- 9.5. Alocar os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;
- 9.6. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;
- 9.7. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o [Código de Defesa do Consumidor \(Lei nº 8.078, de 1990\)](#), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos;
- 9.8. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do fiscal ou gestor do contrato, nos termos do [artigo 48, parágrafo único, da Lei nº 14.133, de 2021](#);
- 9.9. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;
- 9.10. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante;
- 9.11. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.
- 9.12. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.
- 9.13. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.
- 9.14. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.
- 9.15. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.
- 9.16. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.
- 9.17. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;
- 9.18. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;
- 9.19. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação ([art. 116](#));
- 9.20. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas ([art. 116, parágrafo único](#));

9.21. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

9.22. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no [art. 124, II, d, da Lei nº 14.133, de 2021](#);

9.23. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante;

9.24. Realizar os serviços de manutenção e assistência técnica no seguinte local: Av. Pres. Vargas, nº 640 - Campina, Belém - PA, 66017-000

9.24.1. O técnico deverá se deslocar ao local da repartição, salvo se o contratado obtiver sucesso na assistência técnica online, devendo se deslocar após o limite de 2 (dois) requerimentos.

10. CLÁUSULA DÉCIMA- OBRIGAÇÕES PERTINENTES À LGPD

10.1. As partes deverão cumprir a [Lei nº 13.709, de 14 de agosto de 2018 \(LGPD\)](#), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

10.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do [art. 6º da LGPD](#).

10.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

10.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.

10.5. Terminado o tratamento dos dados nos termos do [art. 15 da LGPD](#), é dever do contratado eliminá-los, com exceção das hipóteses do [art. 16 da LGPD](#), incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

10.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

10.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

10.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

10.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

10.10. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados ([LGPD, art. 37](#)), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

10.11. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.

10.12. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

10.13. Os contratos e convênios de que trata o [§ 1º do art. 26 da LGPD](#) deverão ser comunicados à autoridade nacional.

11. CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO (art. 92, XII)

11.1. Não haverá exigência de garantia contratual da execução.

12. CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS (art. 92, XIV)

12.1. Comete infração administrativa, nos termos da [Lei nº 14.133, de 2021](#), o contratado que:

- a) der causa à inexecução parcial do contrato;
- b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c) der causa à inexecução total do contrato;
- d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- f) praticar ato fraudulento na execução do contrato;
- g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

12.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

- i) **Advertência**, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave ([art. 156, §2º, da Lei nº 14.133, de 2021](#));
- ii) **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nas alíneas "b", "c" e "d" do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave ([art. 156, § 4º, da Lei nº 14.133, de 2021](#));
- iii) **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nas alíneas "e", "f", "g" e "h" do subitem acima deste Contrato, bem como nas alíneas "b", "c" e "d", que justifiquem a imposição de penalidade mais grave ([art. 156, §5º, da Lei nº 14.133, de 2021](#)).
- iv) **Multa**:

- (1) Moratória de 10% (dez por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 15 (quinze) dias;
- (2) Compensatória, para as infrações descritas nas alíneas "e" a "h" do subitem 12.1, de 0,5% a 30% do valor do Contrato.
- (3) Compensatória, para a inexecução total do contrato prevista na alínea "c" do subitem 12.1, de 0,5% a 30% do valor do Contrato.
- (4) Para infração descrita na alínea "b" do subitem 12.1, a multa será de 0,5% a 30% do valor do Contrato.
- (5) Para infrações descritas na alínea "d" do subitem 12.1, a multa será de 0,5% a 30% do valor do Contrato.
- (6) Para a infração descrita na alínea "a" do subitem 12.1, a multa será de 0,5% a 30% do valor do Contrato, ressalvadas as seguintes infrações:

- I. Deixar de apresentar um dos itens estabelecidos no item 1.3 deste Termo de Contrato e/ou deixar de dar assistência técnica para a plena operacionalização do equipamento e licença alvo dessa contratação.
- II. Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou consequências letais, por ocorrência; a multa será de até 3,2% ao dia sobre o valor mensal do contrato;
- III. Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais por dia e por unidade de atendimento. A multa será de até 1,6% ao dia sobre o valor mensal do contrato;
- IV. Alocar funcionário sem qualificação para executar os serviços contratados; a multa será de até 0,8% ao dia sobre o valor mensal do contrato;
- V. Recusar-se a executar serviço determinado pela fiscalização, por serviço e por dia; a multa será de até 0,4% ao dia sobre o valor mensal do contrato;
- VI. Deixar de cumprir determinação formal ou instrução complementar do órgão fiscalizador, por ocorrência; a multa será de até 0,4% ao dia sobre o valor mensal do contrato;
- VII. Deixar de cumprir quaisquer dos itens do Aviso de Dispensa e seus Anexos não previstos neste rol de infrações, após reincidência formalmente notificada pelo órgão fiscalizador, por item e por ocorrência; a multa será de até 0,8% ao dia sobre o valor mensal do contrato;
- VIII. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante ([art.](#)

12.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante ([art. 156. §9º. da Lei nº 14.133. de 2021](#))

12.4. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa ([art. 156. §7º. da Lei nº 14.133. de 2021](#)).

12.5. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação ([art. 157. da Lei nº 14.133. de 2021](#).)

12.6. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente ([art. 156. §8º. da Lei nº 14.133. de 2021](#)).

12.7. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

12.8. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no **caput** e parágrafos do [art. 158 da Lei nº 14.133. de 2021](#), para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

12.9. Na aplicação das sanções serão considerados ([art. 156. §1º. da Lei nº 14.133. de 2021](#)):

- a) a natureza e a gravidade da infração cometida;
- b) as peculiaridades do caso concreto;
- c) as circunstâncias agravantes ou atenuantes;
- d) os danos que dela provierem para o Contratante;
- e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

12.10. Os atos previstos como infrações administrativas na [Lei nº 14.133. de 2021](#), ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na [Lei nº 12.846. de 2013](#), serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida [Lei \(art. 159\)](#).

12.11. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia ([art. 160. da Lei nº 14.133. de 2021](#))

12.12. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. ([Art. 161. da Lei nº 14.133. de 2021](#))

12.13. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do [art. 163 da Lei nº 14.133/21](#).

12.14. Os débitos do contratado para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante, na forma da [Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022](#).

13. CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL ([art. 92. XIX](#))

13.1. *O contrato será extinto quando vencido o prazo nele estipulado, salvo disposto no item 2.1.1.*

13.2. *O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o contratante, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.*

13.3. *A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.*

13.4. *Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.*

13.5. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no [artigo 137 da Lei nº 14.133/21](#), bem como amigavelmente, assegurados o contraditório e a ampla defesa.

13.5.1. Nesta hipótese, aplicam-se também os [artigos 138 e 139](#) da mesma Lei.

13.5.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

13.5.3. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

13.6. O termo de extinção, sempre que possível, será precedido:

13.6.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

13.6.2. Relação dos pagamentos já efetuados e ainda devidos;

13.6.3. Indenizações e multas.

13.7. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório ([art. 131. caput, da Lei n.º 14.133. de 2021](#)).

13.8. O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA ([art. 92. VIII](#))

14.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento do Conselho Regional de Contabilidade do Pará, deste exercício, na dotação abaixo discriminada:

I.Gestão/Unidade:

II.Fonte de Recursos:

III.Programa de Trabalho:

IV.Elemento de Despesa:

V.Plano Interno:

VI.Nota de Empenho:

14.2. *A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.*

CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS ([art. 92. III](#))

15.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na [Lei nº 14.133. de 2021](#), e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na [Lei nº 8.078. de 1990 – Código de Defesa do Consumidor](#), – e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos [arts. 124 e seguintes da Lei nº 14.133, de 2021](#).

16.2. O contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

16.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

16.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do [art. 136 da Lei nº 14.133, de 2021](#).

CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

17.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no [art. 94 da Lei 14.133, de 2021](#), bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, *caput*, da Lei n.º 14.133, de 2021, e ao [art. 8º, §2º, da Lei n. 12.527, de 2011](#), c/c [art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012](#).

CLÁUSULA DÉCIMA OITAVA– FORO (art. 92, §1º)

18.1. Fica eleito o Foro da Justiça Federal em, Seção Judiciária de para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme [art. 92, §1º, da Lei nº 14.133/21](#).

[Local], [dia] de [mês] de [ano].

Representante legal do CONTRATANTE

Representante legal do CONTRATADO

TESTEMUNHAS:

1-

2-



Documento assinado eletronicamente por **Gabriela Ramos dos Reis, Assessora**, em 12/09/2024, às 10:56, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Luciano Coutinho Almeida, Analista - Sistemas / Desenvolvimento**, em 01/11/2024, às 16:46, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Newton da Silva Junior, Analista - Sistemas / Desenvolvimento**, em 01/11/2024, às 16:47, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0487261** e o código CRC **7480786D**.